



Dr.WEB

KATANA Business Edition

Manuel administrateur



© **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.

Dr.Web KATANA Business Edition

Version 1.0

Manuel administrateur

20/09/2021

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

1. Introduction	6
1.1. Conventions	6
1.2. Fonctions principales de Dr.Web KATANA Business Edition	7
1.3. Pré-requis système	7
2. Licencing	11
2.1. Réactivation de la licence	11
2.2. Fichier clé	12
3. Installation, récupération et suppression de Dr.Web KATANA Business Edition	13
3.1. Installation de Dr.Web KATANA Business Edition	13
3.2. Récupération et suppression de Dr.Web KATANA Business Edition	14
4. Mise en route	16
5. Gestion des profils	17
6. Préparation des postes	19
7. Configuration du contrôleur de domaine Active Directory	23
8. Recherche des postes et installation de Dr.Web KATANA	25
9. Gestion des postes	28
9.1. Filtre	29
9.2. Options	29
9.2.1. Distribution des clés	30
9.2.2. Redémarrage et arrêt des postes	30
9.2.3. Mise à jour de Dr.Web KATANA	31
9.2.4. Journal des événements	31
9.2.5. Exportation du journal	32
9.2.6. Paramètres de la protection	32
9.2.7. Quarantaine	36
10. Paramètres	38
10.1. Langue du logiciel	39
10.2. Gestion des clés	39
10.3. Paramètres de l'interaction réseau	39
10.4. Configuration des paramètres d'accès au réseau	39
10.5. Mise à jour de Dr.Web KATANA Business Edition	40



11. Gestion des licences

42

12. Annexe A. Méthodes de détection

43




1. Introduction

Cette documentation représente un manuel de l'administrateur de Dr.Web KATANA Edition et contient les informations nécessaires pour l'installation et l'utilisation efficace du logiciel Dr.Web KATANA Business Edition. L'ordre des chapitres correspond à l'ordre d'utilisation du logiciel. Les premiers chapitres décrivent l'installation de Dr.Web KATANA Business Edition, la mise en route, la recherche des postes, l'installation de Dr.Web KATANA sur les postes ; les derniers chapitres décrivent la gestion des paramètres de protection des postes et les paramètres du logiciel Dr.Web KATANA Business Edition.

Ce manuel ne décrit pas la solution antivirus Dr.Web KATANA. Pour obtenir les informations correspondantes, consultez le manuel **Dr.Web KATANA. Manuel utilisateur** ou visitez le [site officiel de la société Doctor Web](#).

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.
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.
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.



1.2. Fonctions principales de Dr.Web KATANA Business Edition

Avec Dr.Web KATANA Business Edition vous pouvez installer Dr.Web KATANA sur les postes du réseau de manière centralisée. Dr.Web KATANA protège les postes contre les menaces informatiques à l'aide des méthodes sans signatures : il analyse le comportement de processus, utilise les technologies cloud de détection des menaces et les règles prédéfinies.

Avec Dr.Web KATANA Business Edition, vous pouvez contrôler le niveau de sécurité des postes et leur statut.

Fonctions principales de Dr.Web KATANA Business Edition :

- installation centralisée de Dr.Web KATANA sur les ordinateurs du réseau ;
- configuration centralisée de Dr.Web KATANA ;
- surveillance des événements viraux et du statut de Dr.Web KATANA sur les postes protégés.

1.3. Pré-requis système

Pour le fonctionnement de Dr.Web KATANA Business Edition, l'ordinateur doit satisfaire aux conditions suivantes :

Composant	Pré-requis
Processeur	Processeur i686 supportant les instructions SSE2.
Mémoire vive disponible	Au moins 100 Mo.
Espace disponible 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">• Windows XP avec Service Pack 3 ou supérieur ;• Windows Vista avec Service Pack 2 ou supérieur ;• Windows 7 ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure ;• Windows Server 2003 avec Service Pack 1 ou supérieur ;• Windows Server 2008 avec Service Pack 2 ou supérieur. Pour les plateformes 64-bits : <ul style="list-style-type: none">• Windows Vista avec Service Pack 2 ou supérieur ;



Composant	Pré-requis
	<ul style="list-style-type: none">• Windows 7 ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure ;• Windows 11;• Windows Server 2008 avec Service Pack 2 ou supérieur ;• Windows Server 2008 R2 ;• Windows Server 2012 ;• Windows Server 2012 R2 ;• Windows Server 2016 ;• Windows Server 2019. <p>Vous aurez peut-être à télécharger et installer les mises à jour pour certains composants système. Si cela est nécessaire, Dr.Web vous indiquera les noms des composants et vous fournira les liens de téléchargement.</p>
Résolution d'écran	La résolution d'écran recommandée doit être au minimum de 1024x768.

Pour un fonctionnement correct de Dr.Web KATANA Business Edition, 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 l'installation de Dr.Web KATANA, les postes (les clients protégés) doivent satisfaire aux conditions suivantes :

Composant	Pré-requis
Processeur	Processeur i686.
Mémoire vive 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.



Composant	Pré-requis
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 ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure ;• Windows Server 2003 avec Service Pack 1 ou supérieur ;• Windows Server 2008. <p>Pour les plateformes 64-bits :</p> <ul style="list-style-type: none">• Windows Vista avec Service Pack 2 ou supérieur ;• Windows 7 ;• Windows 8 ;• Windows 8.1 ;• Windows 10 21H1 ou une version antérieure ;• Windows 11;• Windows Server 2008 avec Service Pack 2 ou supérieur ;• Windows Server 2008 R2 ;• Windows Server 2012 ;• Windows Server 2012 R2 ;• Windows Server 2016 ;• Windows Server 2019. <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 noms de composants et vous fournira les liens de téléchargement.</p>
Résolution d'écran	La résolution d'écran recommandée doit être au minimum de 1024x768.

Pour un fonctionnement correct de Dr.Web KATANA, 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



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



2. Licencing

Pour utiliser Dr.Web KATANA Business Edition, vous devez avoir une licence. Vous pouvez acheter une licence avec le produit sur le [site officiel de Doctor Web](#) ou chez les partenaires.

Activation de la licence

Pour utiliser Dr.Web KATANA Business Edition, il est nécessaire d'activer la licence. Pour ce faire, enregistrez la licence sur le [site officiel de Doctor Web](#) et obtenez un fichier clé. Il est recommandé d'activer la licence avant d'installer Dr.Web KATANA Business Edition. Dans ce cas, vous pourrez spécifier le fichier clé lors de l'installation et commencer le travail juste après la fin de l'installation du logiciel. Sinon, il sera impossible d'utiliser Dr.Web KATANA Business Edition jusqu'à ce que vous spécifiez le fichier clé.

Prix de la licence

Le prix de la licence pour l'utilisation de Dr.Web KATANA Business Edition dépend du nombre de postes dans le réseau sur lesquels il faut installer Dr.Web KATANA. L'ordinateur de l'administrateur du réseau est pris en compte si vous installez sur cet ordinateur non seulement Dr.Web KATANA Business Edition, mais aussi Dr.Web KATANA. L'installation de Dr.Web KATANA sur l'ordinateur d'administrateur s'effectue à l'aide de Dr.Web KATANA Business Edition depuis la section du logiciel **Installation**.

Achat d'une nouvelle licence

Si lors de l'utilisation de Dr.Web KATANA Business Edition, il vous faudra installer Dr.Web KATANA sur un plus grand nombre de postes, vous pourrez acheter une nouvelle licence sur le [site officiel de Doctor Web](#) ou chez les partenaires. Avec la nouvelle licence, vous pourrez installer Dr.Web KATANA sur de nouveaux postes et continuer à gérer les postes sur lesquels Dr.Web KATANA a été déjà installé. Dans ce cas, la licence précédente sera bloquée.

L'installation de Dr.Web KATANA est possible uniquement sur le nombre de postes indiqué dans la licence valide.

2.1. Réactivation de la licence

Vous pouvez avoir à réactiver votre licence en cas de perte du fichier clé.



Lors 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, 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 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 logiciel. Le fichier clé vous sera envoyé par le service de support technique à votre adresse e-mail.

2.2. Fichier clé

Les droits d'utilisation de Dr.Web sont enregistrés dans le fichier spécial dit le *fichier clé*. Le fichier clé possède l'extension `.key` et contient les informations suivantes :

- la liste des composants que l'utilisateur est autorisé à utiliser ;
- la période pendant laquelle l'utilisateur est autorisé à utiliser le logiciel ;
- la disponibilité du support technique ;
- d'autres restrictions (notamment, le nombre d'ordinateurs sur lesquels il est autorisé d'utiliser l'antivirus).



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

En cas d'absence du fichier clé valide, Dr.Web KATANA Business Edition ne va pas fonctionner.

Un fichier clé de Dr.Web *valide* satisfait en même temps 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 pendant toute la durée de validité de la licence.



3. Installation, récupération et suppression de Dr.Web KATANA Business Edition

Avant d'installer Dr.Web KATANA Business Edition, il est fortement recommandé de consulter les [pré-requis système](#), ainsi que :

- d'installer toutes les mises à jour critiques créées par Microsoft pour votre système d'exploitation (en savoir plus sur la mise à jour de [Windows](#) et [Windows Server](#)). Si le système d'exploitation n'est plus supporté, migrez vers une nouvelle version du système d'exploitation ;
- d'analyser le système de fichiers et de résoudre les problèmes détectés ;
- de fermer toutes les applications en cours.

3.1. Installation de Dr.Web KATANA Business Edition

Pour installer Dr.Web KATANA Business Edition

1. Lancez le fichier d'installation que vous avez obtenu lors de l'achat de la licence.
2. Consultez le contrat de licence. Pour ce faire, cliquez sur le lien correspondant dans la première fenêtre.
3. Pour spécifier le chemin d'installation et certains paramètres supplémentaires, cliquez sur **Paramètres d'installation**. Si vous voulez effectuer l'installation avec les paramètres par défaut, passez à l'étape 4.
 - Dans le premier onglet, vous pouvez sélectionner le chemin d'installation.
 - Dans l'onglet **Options avancées**, vous pouvez configurer la création des raccourcis pour lancer le logiciel.

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 **Licence** qui s'affiche :
 - sélectionnez **Spécifier le chemin d'accès au fichier clé valide** si vous possédez un fichier clé sur un disque dur ou sur un support amovible. Cliquez sur **Parcourir** et sélectionnez le fichier clé dans la fenêtre d'ouverture de fichier ;
 - sélectionnez **Obtenir le fichier clé plus tard** pour continuer l'installation sans fichier clé. Dans ce cas, il est impossible d'utiliser le programme jusqu'à ce que vous spécifiez le fichier clé valide.

Cliquez le bouton **Installer** pour lancer le processus d'installation.
6. Après la fin de l'installation, activez l'option **Lancer Dr.Web KATANA Business Edition** pour lancer KATANA Business Edition.



Actions effectuées après l'installation de Dr.Web KATANA Business Edition

Si un pare-feu tiers est installé sur l'ordinateur de l'administrateur du réseau :

- ajoutez le fichier `dwservice.exe` aux exclusions du pare-feu. Le port UDP utilisé doit avoir le numéro 55567, le numéro du port TCP est aléatoire.

Si un pare-feu tiers est installé sur les ordinateurs du réseau :

- ajoutez le fichier `katana-console.exe` aux exclusions du pare-feu sur chaque ordinateur avec Dr.Web KATANA installé. Les numéros des ports UDP et TCP utilisés sont aléatoires.

Installation de Dr.Web KATANA sur l'ordinateur de l'administrateur du réseau

Outre Dr.Web KATANA Business Edition, vous pouvez installer Dr.Web KATANA sur votre ordinateur. Pour ce faire, ouvrez la section **Installation** après le lancement de Dr.Web KATANA Business Edition et continuez l'installation de Dr.Web KATANA sur votre ordinateur et l'installation de Dr.Web KATANA sur les autres postes.

Pour plus d'informations sur l'installation de Dr.Web KATANA sur le poste, consultez le chapitre [Installation de Dr.Web KATANA sur le poste](#).

3.2. Récupération et suppression de Dr.Web KATANA Business Edition

1. Pour supprimer ou récupérer Dr.Web KATANA Business Edition, sélectionnez (en fonction du système d'exploitation) :
 - sous Windows XP (en fonction de l'affichage du menu Démarrer) :
 - Menu Démarrer : Démarrer → Panneau de configuration → Ajout/suppression de programmes.
 - Menu classique Démarrer : Démarrer → Paramètres → Panneau de configuration → Ajout/suppression de programmes.
 - sous Windows Vista (en fonction de l'affichage du menu Démarrer) :
 - Menu Démarrer : Démarrer → Panneau de configuration, puis selon l'affichage du Panneau de configuration :
 - Affichage classique : Programmes et fonctionnalités.
 - Page d'accueil : Programmes → Programmes et fonctionnalités.
 - Menu classique Démarrer : Démarrer → Paramètres → Panneau de configuration → Programmes et fonctionnalités.
 - sous Windows 7, sélectionnez Démarrer → Panneau de configuration, puis selon l'affichage du Panneau de configuration :
 - Petites/grandes icônes : Programmes et fonctionnalités.
 - Catégorie : Programmes → Suppression de programmes.



- sous Windows 8, Windows 8.1 et Windows 10, ouvrez le Panneau de configuration, par exemple, via l'élément Panneau de configuration dans le menu contextuel qui peut être affiché avec un clic droit dans le coin inférieur gauche du bureau. Puis selon le type de l'élément Affichage du Panneau de configuration :
 - Petites/grandes icônes : Programmes et fonctionnalités.
 - Catégorie : Programmes → Suppression de programmes.
- 2. Dans la liste qui apparaît, sélectionnez la ligne affichant le nom du programme. Pour récupérer ou supprimer le programme, cliquez sur le bouton nécessaire.
- 3. Dans la fenêtre **Paramètres sauvegardés**, vous serez invité à enregistrer les paramètres des profils qui peuvent être utilisés par le programme lors de la réinstallation. Cette option est sélectionnée par défaut.



4. Mise en route

Si lors de l'installation de Dr.Web KATANA Business Edition, vous avez spécifié un fichier clé valide, vous pouvez commencer le travail juste après le lancement du programme. Si le fichier clé n'a pas été spécifié, spécifiez le fichier clé valide au démarrage du programme pour continuer à utiliser Dr.Web KATANA Business Edition.

Pour commencer à gérer les postes

1. [Créez un profil.](#)
2. [Préparez les postes](#) à l'installation de Dr.Web KATANA.
3. [Ajoutez les postes.](#)
4. [Installez Dr.Web KATANA](#) sur les postes.

A mesure que Dr.Web KATANA s'installe, les postes apparaissent dans la liste de la section **Gestion**. Vous pouvez ouvrir cette section et commencer à gérer les postes de la liste même si l'installation de Dr.Web KATANA n'est pas terminée sur certains postes. Les postes apparaissent dans la section **Gestion** automatiquement à la fin de l'installation de Dr.Web KATANA.



5. Gestion des profils

La gestion de Dr.Web KATANA Business Edition est possible uniquement si vous avez un profil où sont enregistrés les clés, les identifiants d'accès au réseau et les configurations de Dr.Web KATANA Business Edition. Aux prochains lancements du logiciel, vous pouvez vous connecter au profil existant ou créer un nouveau profil.


Pour créer un nouveau profil au lancement du programme

1. Cliquez sur le bouton **Commencer le travail** dans la fenêtre d'accueil.
2. Dans la fenêtre qui s'affiche, spécifiez le nom du profil et le mot de passe.
3. Créez les clés de chiffrement pour votre profil. Vous pouvez générer les clés automatiquement ou télécharger une clé privée existante. Dans ce dernier cas, la clé publique sera générée automatiquement.
4. Après la création du nouveau profil, la section **Installation** va s'ouvrir. Dans cette section, vous pouvez [trouver les postes et installer](#) Dr.Web KATANA sur ces postes.




La création des clés de chiffrement est obligatoire pour chaque profil. Une seule paire de clés peut être enregistrée. Plus tard, vous pourrez [créer](#) de nouvelles clés de chiffrement et les [distribuer](#) sur les postes si cela est nécessaire.

Pour vous connecter à un profil existant

1. Sélectionnez le nom du profil nécessaire dans la liste **Nom d'utilisateur**.
2. Entrez le mot de passe. Pour voir le mot de passe, cliquez sur .
3. Cliquez sur le bouton **Se connecter**.

Pour créer un nouveau profil depuis la fenêtre principale du programme


Si vous voulez créer un nouveau profil pendant votre gestion du logiciel

1. Cliquez sur  contre l'élément du menu **Profils**.
2. Dans la fenêtre qui s'affiche, spécifiez le nom du profil et le mot de passe.
3. Créez les clés de chiffrement pour votre profil. Vous pouvez les générer automatiquement avec Dr.Web KATANA Business Edition ou charger une clé privée existante. Dans ce dernier cas, la clé publique sera générée automatiquement.

L'option **Importer les paramètres actuels dans un nouveau profil** permet d'importer les paramètres et les clés de chiffrement depuis le profil que vous utilisez en ce moment. Tous les paramètres sont importés dans le nouveau profil, y compris les paramètres que vous n'avez pas encore enregistrés. L'option est activée par défaut.

Vous pouvez changer des profils existants dans le menu latéral.



Vous pouvez également supprimer les profils. Pour ce faire, placez le curseur sur le nom du profil dans le menu latéral et cliquez sur . Si vous supprimez le profil que vous utilisez pour gérer les postes, vous pouvez vous connecter à un des postes existants ou créer un nouveau profil.



6. Préparation des postes

Pour installer Dr.Web KATANA sur les postes, il est nécessaire de satisfaire à toutes les conditions suivantes :

- l'option **Découverte de réseau** doit être activée sur l'ordinateur sur lequel est lancé Dr.Web KATANA Business Edition, si vous comptez rechercher les postes par ce moyen ;
- l'ordinateur distant doit être accessible via le réseau ;
- le compte sous lequel s'effectue la connexion doit être opérationnel et avoir assez de privilèges ;
- si l'ordinateur distant est protégé par un pare-feu, les paramètres avancés doivent être configurés.

Si vous utilisez le pare-feu Windows, ouvrez l'onglet **Paramètres avancés** dans ses paramètres, sélectionnez **Règles de trafic entrant** et activez les exclusions suivantes : **Service Accès réseau (NP-In)** et **Partage de fichiers et d'imprimantes (SMB-In)**. Les exclusions pour le profil du pare-feu **Private** doivent être activées. Si le poste se trouve dans le domaine, les exclusions pour le profil **Domain** doivent être activées.

Si vous utilisez d'autres pare-feux, il faut ouvrir le port 445 ;

- il est nécessaire d'effectuer une configuration supplémentaire (voir ci-dessous).

Avant de procéder à l'installation, assurez-vous d'avoir toutes les informations nécessaires sur les identifiants d'administrateurs sur tous les postes.



Toutes les étapes de préparation du système d'exploitation du poste doivent être réalisées en mode administrateur.

Configuration supplémentaire

Pour installer Dr.Web KATANA sur les postes, il est nécessaire de satisfaire simultanément aux conditions supplémentaires suivantes :

- Les restrictions du système de contrôle de comptes utilisateur (UAC) doivent être désactivées, si le poste fonctionne sous Windows Vista ou un système d'exploitation supérieur. Si vous utilisez le compte administrateur intégré, la configuration de ce paramètre n'est pas requise. Passez à l'étape suivante.

Ouvrez l'éditeur de registre du système d'exploitation.

1. Trouvez et sélectionnez la branche suivante
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.
2. Si la clé **LocalAccountTokenFilterPolicy** n'est pas présente dans la branche, créez-la :
 - a. Dans le menu **Édition**, sélectionnez la commande **Créer**, puis **Valeur DWORD**.
 - b. Entrez le nom de la clé **LocalAccountTokenFilterPolicy**.



3. Dans le menu contextuel de la clé **LocalAccountTokenFilterPolicy**, sélectionnez **Modifier**.
4. Dans le champ **Valeur**, saisissez **1**.
5. Appuyez sur **OK** et quittez l'éditeur.
6. Redémarrez la machine.
7. Reproduisez la procédure pour tous les postes à scanner.



Cette opération doit être effectuée par l'administrateur ou par un utilisateur expérimenté. Une fausse manoeuvre lors de la modification du registre peut endommager le système. Les spécialistes de Microsoft recommandent de créer une copie de sauvegarde des données importantes conservées sur l'ordinateur avant de procéder à la modification du registre.

- Tous les services requis pour le fonctionnement du réseau doivent être installés et configurés ;

Vérification de la configuration réseau

1. Ouvrez le Panneau de configuration sur le poste.
 - Lorsque vous configurez les systèmes supportés antérieurs à Windows Vista, sélectionnez la rubrique **Connexions réseau** (si la rubrique n'est pas affichée, cliquez sur le bouton **Basculer vers l'affichage classique**).
 - Lorsque vous configurez Windows Vista, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Afficher l'état et la gestion du réseau** → **Gérer les connexions réseau**.
 - Lorsque vous configurez Windows 7 ou Windows Server 2008, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Afficher l'état et la gestion du réseau** → **Modifier les paramètres de la carte**.
 - Lorsque vous configurez Windows 8, Windows 10 ou Windows Server 2012, dans la catégorie **Réseau et Internet** sélectionnez **Centre Réseau et partage** → **Modifier les paramètres de la carte**.
 2. Cliquez droit sur la connexion nécessaire et sélectionnez l'élément **Propriétés**.
 3. Vérifiez que les services suivants sont installés et configurés pour la connexion sélectionnée :
 - client pour les réseaux Microsoft ;
 - service du partage de fichiers et d'imprimantes pour les réseaux Microsoft ;
 - protocole Internet en version 4 (TCP/IPv4) ou en version 6 (TCP/IPv6).
 4. Enregistrez les modifications et fermez la fenêtre de configuration.
- Les paramètres de partage doivent autoriser la configuration avancée.

Configuration du partage

1. Ouvrez le Panneau de configuration sur le poste.



- Lorsque vous configurez Windows XP ou Windows Server 2003, sélectionnez l'élément **Pare-feu Windows** (si la section n'est pas présente, cliquez sur **Basculer vers l'affichage classique**).
 - Lorsque vous configurez Windows Vista, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Configuration du partage de fichiers**.
 - Lorsque vous configurez Windows 7 ou Windows Server 2008, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Réseau et Internet**, sélectionnez **Centre Réseau et partage**, puis sélectionnez **Modifier les paramètres de partage avancés**.
 - Lorsque vous configurez Windows 8, Windows 10 ou Windows Server 2012, dans la catégorie **Réseau et Internet**, sélectionnez **Centre Réseau et partage**, puis sélectionnez **Modifier les paramètres de partage avancés**.
2. Dans la fenêtre qui s'affiche, effectuez une des actions suivantes :
 - Si vous configurez Windows XP ou Microsoft Windows Server 2003, passez à l'onglet **Exclusions** et activez le paramètre **Partage de fichiers et d'imprimantes**.
 - Si vous configurez Windows Vista, activez **Recherche du réseau** et sélectionnez **Partage de fichiers**.
 - Si vous configurez Windows 7, sélectionnez **Activer la découverte de réseau** et **Activer le partage de fichiers et d'imprimantes**.
 - Si vous configurez Microsoft Windows Server 2008, Windows 8, Windows 10 ou Microsoft Windows Server 2012, sélectionnez **Activer le partage de fichiers et d'imprimantes**.
 3. Enregistrez les modifications et fermez la fenêtre de configuration.
- Pour les comptes locaux, il faut utiliser le modèle standard de partage et de sécurité.

Configuration d'un modèle de partage et de sécurité

1. Ouvrez le Panneau de configuration sur le poste.
 - Lorsque vous configurez des systèmes pris en charge antérieurs à Windows Vista, sélectionnez l'élément **Administration** (si la rubrique n'est pas affichée, cliquez sur le bouton **Basculer vers l'affichage classique**) et lancez l'utilitaire **Stratégie de sécurité locale**.
 - Lorsque vous configurez Windows Vista ou des systèmes supérieurs, sélectionnez le mode d'affichage par catégorie. Dans la catégorie **Système et sécurité**, sélectionnez le groupe **Administration** et lancez l'utilitaire **Stratégie de sécurité locale**.



Pour lancer l'utilitaire de configuration des politiques de sécurité locales, vous pouvez saisir dans le champ de recherche Windows la commande `secpol.msc`, puis cliquer sur ENTRÉE.

2. Dans l'arborescence de la console, sélectionnez le groupe **Stratégies locales**, puis — le groupe **Paramètres de sécurité**.



3. Cliquez droit sur le paramètre **Accès réseau : modèle de partage et de sécurité pour les comptes locaux**, sélectionnez l'élément **Propriétés** et définissez la valeur **Classique — les utilisateurs locaux s'authentifient eux-mêmes**.



Par défaut, une connexion à un poste distant peut être établie à condition que le compte utilisé soit protégé par un mot de passe qui n'est pas vide. Pour vous connecter, spécifiez un mot de passe non vide.

4. Fermez la console.



7. Configuration du contrôleur de domaine Active Directory

Si l'organisation utilise le contrôleur de domaine Active Directory, il est nécessaire de configurer :

- les paramètres du partage de fichiers et d'imprimantes ;
- les paramètres de sécurité.

Vous pouvez créer un nouvel objet de stratégie de groupe (GPO) pour appliquer ces paramètres ou modifier les paramètres d'un objet existant.

Pour créer un nouvel objet de stratégie de groupe

1. Entrez `gpmmc.msc` dans le champ de la fenêtre de ligne de commande et lancez la console de gestion des stratégies de groupe **GPMC**.
2. Créez un nouvel objet de stratégie de groupe, par exemple **GPO-KATANABUSINESSEDITION**. Pour ce faire, cliquez droit sur **Objets de stratégie de groupe** dans l'arborescence de la console **GPMC** de la forêt et du domaine correspondants. Cliquez sur **Créer**. Dans la fenêtre qui s'affiche, indiquez un nouveau nom de l'objet et cliquez sur **OK**.
3. Attachez l'objet créé au domaine nécessaire.
4. Cliquez droit sur l'objet créé, sélectionnez **Modifier** et corrigez les paramètres nécessaires conformément à la description ci-dessous.

Si vous avez décidé de ne pas créer un nouvel objet, mais de modifier les paramètres d'un objet existant, ouvrez la fenêtre des paramètres correspondants.

1. Sur l'ordinateur sur lequel la console de gestion des stratégies de groupe GPMC est installée, cliquez sur **Démarrage** → **Outils d'administration** → **Gestion des stratégies de groupe**.
2. Si la fenêtre de contrôle de comptes s'affiche, vérifiez les données et cliquez sur **Continuer**.
3. Dans la zone de navigation trouvez le noeud **Forêt : Nom de la forêt** et développez-le, puis développez le noeud **Objets de stratégie de groupe** et cliquez droit sur le nom de l'objet pour lequel vous voulez spécifier l'autorisation.
4. Dans le menu qui s'affiche, sélectionnez **Modifier**.

Configuration du partage de fichiers et d'imprimantes

Autorisez les requêtes entrantes d'ordinateurs client pour l'accès aux fichiers. L'activation de cette exception du pare-feu ouvre les ports UDP 137 et 138 et le port TCP 445 pour les adresses IP indiquées dans cette règle.



Dans la zone de navigation de la fenêtre affichée, développez les noeuds suivants

1. Dans la zone de navigation de la fenêtre affichée, développez les noeuds suivants : **Configuration ordinateur** → **Stratégies** → **Modèles d'administration** → **Réseau** → **Connexions réseau** → **Pare-feu Windows** → **Profil du domaine**.
2. Dans la zone de notification double-cliquez sur le paramètre **Pare-feu Windows : Autorise l'exception de partage de fichiers et d'imprimantes** et activez cette règle dans l'onglet de paramètres.
3. Dans le champ **Autoriser des messages entrants non-requis de ces adresses IP**, spécifiez une plage nécessaire.
4. Cliquez sur **OK** pour enregistrer les modifications.

Configuration des paramètres de sécurité

Configurez la stratégie **Accès réseau : modèle de partage et de sécurité pour les comptes locaux** de sorte qu'au moment de connexion au réseau avec les données du compte local, le contrôle d'authenticité s'effectue conformément à ces données.

Autorisation d'accès réseau via les comptes locaux d'utilisateurs

1. Dans la zone de navigation de la fenêtre affichée, développez les noeuds suivants : **Configuration Ordinateur** → **Stratégies** → **Configuration Windows** → **Paramètres de sécurité** → **Stratégies locales** → **Paramètres de sécurité**.
2. Définissez la valeur **Classique — les utilisateurs locaux s'authentifient eux-mêmes** pour la stratégie **Accès réseau : modèle de partage et de sécurité pour les comptes locaux**.

Application des modifications dans le domaine

Pour appliquer les modifications de stratégies de groupe dans le domaine, dans les deux cas (lors de la création d'un nouvel objet et lors de la modification d'un objet existant) entrez la commande `gpupdate /force` dans la fenêtre de la ligne de commande.



8. Recherche des postes et installation de Dr.Web KATANA

Pour commencer à gérer les postes et régler le niveau de leur protection, il vous faut rechercher des postes et installer Dr.Web KATANA sur ces postes.



Les postes connectés doivent faire partie du même segment de réseau dans lequel Dr.Web KATANA Business Edition est installé

Si vous n'avez pas assez de droits pour accéder au réseau, vous verrez une notification correspondante. Pour installer Dr.Web KATANA avec succès, dans la rubrique [Paramètres](#), entrez le nom d'utilisateur et le mot de passe pour accéder au réseau ou redémarrez Dr.Web KATANA Business Edition avec les droits d'administrateur. Sinon l'installation de Dr.Web KATANA sur le poste peut échouer.

Recherche des postes et installation de Dr.Web KATANA

1. Dans la rubrique de programme **Installation** cliquez sur **Ajouter des postes**.
2. Dans la fenêtre d'ajout des postes, sélectionnez le mode de recherche des postes :
 - recherche du réseau ;
 - recherche dans Active Directory ;
 - ajout manuel des postes (vous pouvez entrer l'adresse IP du poste ou son nom réseau, ainsi que la plage des adresses IP des postes avec un trait d'union (« - ») ou avec un masque).
3. Cliquez sur le bouton **Rechercher les postes** pour commencer la recherche des postes. Une fois tous les postes disponibles trouvés, la recherche se termine automatiquement. Vous pouvez arrêter la recherche en cliquant sur **Arrêter la recherche**. Dans ce cas, tous les postes trouvés à ce moment sont enregistrés dans la liste.
4. Une fois la recherche terminée, sélectionnez les postes nécessaires dans la liste et cliquez sur le bouton **Installer KATANA**.
5. La fenêtre d'installation de Dr.Web KATANA contenant la liste des postes s'affiche. Cette liste est sauvegardée dans la rubrique **Installation** jusqu'au redémarrage de Dr.Web KATANA Business Edition.



L'installation de Dr.Web KATANA est possible uniquement sur le nombre de postes autorisé par la licence valide.

Dr.Web KATANA s'installe automatiquement. A la fin de l'installation, les postes apparaissent dans la liste de la rubrique **Gestion**. Vous pouvez ouvrir cette rubrique et commencer à gérer les postes de la liste même si l'installation Dr.Web KATANA n'est pas terminée sur certains postes. Les postes apparaissent dans la rubrique **Gestion** automatiquement.



Si parmi les postes sélectionnés, il y a ceux sur lesquels la version autonome de Dr.Web KATANA est déjà installée, la nouvelle installation ne sera pas effectuée. Ces postes apparaîtront automatiquement dans la liste de la rubrique **Gestion**. Pour commencer à gérer ces postes, [distribuez](#) sur les postes la clé publique utilisée.

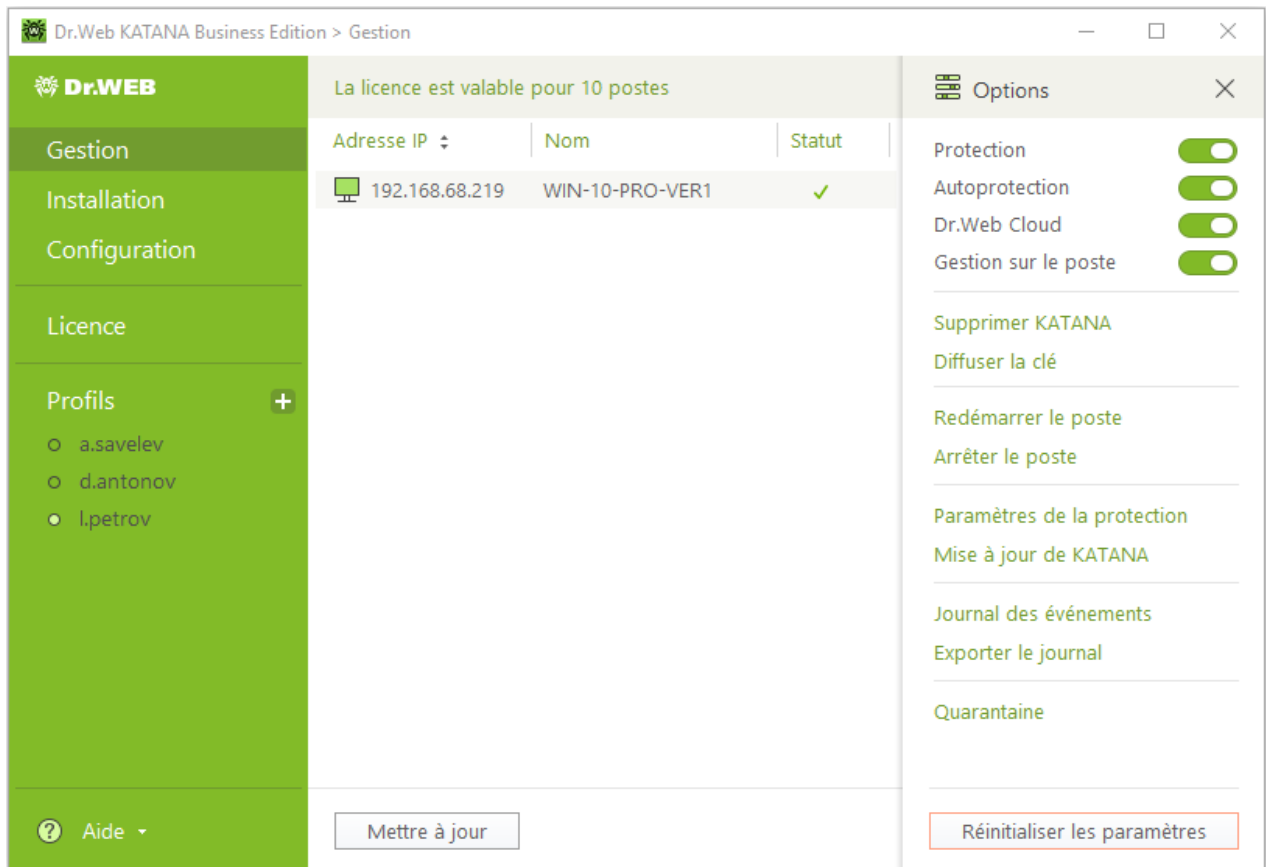






Figure 1. Gestion des postes

Liste des postes

La liste de la rubrique **Installation** comprend trois colonnes : **Adresse IP**, **Nom** et **Statut**. Si cela est nécessaire vous pouvez trier la liste par une des colonnes. L'icône de poste dans la colonne **Adresse IP** affiche les statuts suivants de l'installation :

-  : l'installation est terminée avec succès ;
-  : Dr.Web KATANA s'installe en mode standard ;
-  : l'installation s'est terminée avec une erreur. Pour plus d'informations sur l'erreur, double-cliquez sur .

Pour configurer l'affichage des postes dans la liste, sélectionnez le paramètre de filtrage nécessaire dans le menu déroulant en bas de la fenêtre.

Réinstaller. Cliquez sur ce bouton pour reprendre la tentative d'installation de Dr.Web KATANA sur un ou plusieurs postes, si l'installation sur ces postes a échoué.



Ajouter des postes. Cliquez sur ce bouton pour ajouter de nouveaux postes aux postes de la liste.

Si vous rencontrez des difficultés lors de l'installation de Dr.Web KATANA sur le poste, vous pouvez consulter l'Aide du logiciel en ouvrant la rubrique **Aide**. Cette rubrique se trouve dans la barre latérale du programme.



9. Gestion des postes

Dans la rubrique **Gestion**, vous pouvez gérer les paramètres des postes sur lesquels est installé Dr.Web KATANA, régler le niveau de protection et consulter le statut des composants de Dr.Web KATANA sur les postes sélectionnés. Vous pouvez commencer à gérer les postes même si l'installation de Dr.Web KATANA n'est pas terminée sur tous les postes. Les autres postes seront affichés automatiquement dans la liste de la rubrique **Gestion**. Pour configurer l'[affichage des postes](#) dans la liste, cliquez sur . Pour ouvrir les [paramètres du poste](#), cliquez sur .

Liste des postes


La liste comprend trois colonnes : **Adresse IP**, **Nom** et **Statut**. Si cela est nécessaire vous pouvez trier la liste par une des colonnes. La colonne **Adresse IP** affiche le statut du poste, la colonne **Statut** affiche les informations sur le fonctionnement de Dr.Web KATANA sur le poste. Ces colonnes peuvent contenir les informations suivantes :

Adresse IP	Statut
: le poste est disponible pour la gestion.	<p>Statuts possibles</p> <ol style="list-style-type: none">✓ : le poste est bien protégé ;⚠ : le poste n'est pas complètement protégé par une des raisons suivantes :<ul style="list-style-type: none">• l'autoprotection est désactivée ;• la protection préventive est désactivée ;• les mises à jour automatiques sont désactivées ;• la licence a expiré ;• le redémarrage du poste est requis. <p>Cliquez sur pour apprendre le statut de fonctionnement de Dr.Web KATANA sur le poste sélectionné. Pour fournir une protection optimale, il est recommandé d'activer les composants nécessaires ou redémarrer le poste, si cela est nécessaire.</p>
: le poste est indisponible pour la gestion.	<p>⚠ : le poste n'est pas protégé car une nouvelle clé publique n'a pas été distribuée sur ce poste (pour plus d'informations, voir Gestion des clés).</p> <p>Pour distribuer une nouvelle clé</p> <ol style="list-style-type: none">Vérifiez que toutes les exigences de la section Préparation des postes sont respectées.Sélectionnez un ou plusieurs postes.Ouvrez le panneau Options et cliquez sur le bouton Distribuer la clé.




Seuls les postes en ligne sont affichés dans la liste. Les postes hors ligne ou les postes en redémarrage ne sont pas affichés dans la liste. Dr.Web KATANA Business Edition actualise la liste des postes automatiquement. Si nécessaire, vous pouvez forcer l'actualisation de la liste des postes en cliquant sur le bouton **Mettre à jour**.

9.1. Filtre

Pour configurer les paramètres de filtrage pour la liste de postes, cliquez sur . La liste de postes change automatiquement en fonction des paramètres sélectionnés. Si vous fermez la barre latérale, les paramètres de filtrage spécifiés sont enregistrés jusqu'à ce que vous quittiez le programme.

9.2. Options

Pour modifier les paramètres pour les postes sélectionnés, cliquez sur . Si vous fermez la barre latérale, les paramètres spécifiés seront enregistrés. Certaines configurations peuvent être appliquées à plusieurs postes en même temps.

Paramètres de la protection des postes

- **Protection.** Activer ou désactiver la protection Dr.Web KATANA sur le poste. La configuration peut être appliquée uniquement à un seul poste.
- **Autoprotection.** Activer ou désactiver la protection de fichiers et de processus Dr.Web KATANA sur le poste sélectionné contre l'influence non autorisée et l'endommagement accidentel. La configuration peut être appliquée uniquement à un seul poste.
- **Dr.Web Cloud.** Autoriser ou interdire la connexion au service cloud de la société Doctor Web et au programme d'amélioration de la qualité des produits Dr.Web. 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. La configuration peut être appliquée uniquement à un seul poste.
- **Gestion sur le poste.** Autoriser ou interdire la gestion locale de Dr.Web KATANA. Si cette option est désactivée, l'utilisateur ne peut pas gérer les paramètres de Dr.Web KATANA, car ils seront inactifs. La configuration peut être appliquée uniquement à un seul poste.

Paramètres avancés de la protection des postes

- **Supprimer KATANA.** Supprimer Dr.Web KATANA sur un ou plusieurs postes.
- **Distribuer la clé.** [Distribuer une nouvelle clé publique](#) sur un ou plusieurs postes.
- **Paramètres de la protection.** [Configurer la réaction de Dr.Web KATANA](#) à des actions d'autres applications qui pourraient compromettre la sécurité de votre poste et choisir le niveau de la protection contre les exploits. La configuration peut être appliquée uniquement à un seul poste.



- **Mise à jour de KATANA.** [Spécifier les paramètres de la mise à jour de Dr.Web KATANA](#) sur le poste. La configuration peut être appliquée uniquement à un seul poste.
- **Quarantaine.** Consulter [le contenu de la quarantaine](#) sur le poste sélectionné qui sert à isoler les fichiers suspectés d'être malveillant. La configuration peut être appliquée uniquement à un seul poste.

Paramètres du fonctionnement des postes

- **Redémarrer le poste.** [Redémarrer](#) un ou plusieurs postes sélectionnés.
- **Arrêter les poste.** [Arrêter](#) un ou plusieurs postes sélectionnés.

Paramètres du journal des événements

- **Journal des événements.** Ouvrir la fenêtre contenant les [informations détaillées sur le fonctionnement de Dr.Web KATANA](#) sur le poste sélectionné. La configuration peut être appliquée uniquement à un seul poste.
- **Exporter le journal.** [Sauvegarder les journaux des événements](#) d'un ou de plusieurs postes sélectionnés.

9.2.1. Distribution des clés

Après la création ou téléchargement de nouvelles clés de chiffrement dans la rubrique [Paramètres](#), il est nécessaire de les distribuer sur les postes. Sinon, vous ne pourrez pas continuer à gérer les postes.



Si vous travaillez dans les profils utilisant l'ancienne clé, vous ne pourrez pas gérer les postes sur lesquels la nouvelle clé publique de chiffrement a été envoyée.

Pour distribuer les nouvelles clés de chiffrement

1. Vérifiez que toutes les exigences de la section [Préparation des postes](#) sont respectées.
2. Sélectionnez un ou plusieurs postes possédant une licence valide.
3. Cliquez sur le bouton **Distribuer la clé**.

9.2.2. Redémarrage et arrêt des postes

Pour redémarrer ou arrêter les postes

1. Sélectionnez un ou plusieurs postes possédant une licence valide.
2. Cliquez sur le bouton **Redémarrer le poste** ou **Arrêter les poste**.
3. Dans la fenêtre qui s'affiche, sélectionnez un délai dans lequel les postes seront redémarrés ou arrêtés.



4. Si nécessaire, dans le champ **Message**, entrez le texte à afficher à l'utilisateur avant l'exécution d'une action sélectionnée.

9.2.3. Mise à jour de Dr.Web KATANA

Périodicité des mises à jour. Spécifiez la fréquence de la vérification de la disponibilité des mises à jour de Dr.Web KATANA. La valeur par défaut (30 minutes) est optimale pour maintenir à jour les informations sur les menaces.


Utiliser un serveur proxy Activez cette option si vous voulez utiliser le serveur proxy lors de la mise à jour et spécifiez les paramètres de connexion à ce serveur.

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Nom d'utilisateur	Spécifiez le nom du compte pour la connexion au serveur proxy.
Mot de passe	Spécifiez le mot de passe du compte utilisé pour la connexion au serveur proxy.
Type d'authentification	Sélectionnez le type d'authentification nécessaire pour la connexion au serveur proxy.


9.2.4. Journal des événements

Dans cette fenêtre, vous pouvez consulter les informations détaillées sur le fonctionnement de Dr.Web KATANA sur le poste sélectionné. Le journal des événements contient les informations sur le statut des composants de Dr.Web KATANA. En cas d'erreurs ou d'avertissements sur le fonctionnement de Dr.Web KATANA, ils sont également affichés dans le journal des événements.

Filtre

Pour configurer les paramètres de filtrage des événements, cliquez sur . La liste de postes change automatiquement en fonction des paramètres de filtrage sélectionnés. Si vous fermez la barre latérale, les paramètres de filtrage spécifiés sont enregistrés jusqu'à ce que vous quittiez le programme.

Options

Si vous cliquez sur , la barre latérale s'ouvre et donne accès aux paramètres avancés du journal des événements. Cette barre vous fournit les fonctionnalités suivantes :



- **Afficher les détails.** Si vous activez cette option les informations détaillées pour l'événement sélectionné seront affichées dans une fenêtre supplémentaire. L'option est activée par défaut.
- **Exporter le journal.** Quand vous cliquez sur ce bouton, vous pouvez sauvegarder le journal des événements pour le poste sélectionné. Dans la fenêtre qui s'affiche, sélectionnez le format de fichier, les paramètres de filtrage des événements et le chemin d'enregistrement du fichier.
- **Effacer le journal.** Quand vous cliquez sur ce bouton, tous les enregistrements des événements sur le poste sélectionné seront supprimés.

9.2.5. Exportation du journal

Pour exporter le journal des événements

1. Sélectionnez les postes pour lesquels il faut sauvegarder le journal des événements et cliquez sur **Exporter le journal**.
2. Dans la fenêtre qui s'affiche, sélectionnez le format de fichier, le type et la période des événements ainsi que le chemin d'enregistrement du fichier de journal.

Si vous voulez sauvegarder le fichier du journal pour un seul poste ou que vous avez spécifié les paramètres de filtrage des événements pour ce poste dans la [fenêtre des paramètres](#) du Journal des événements, ces paramètres sont enregistrés.

9.2.6. Paramètres de la protection

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

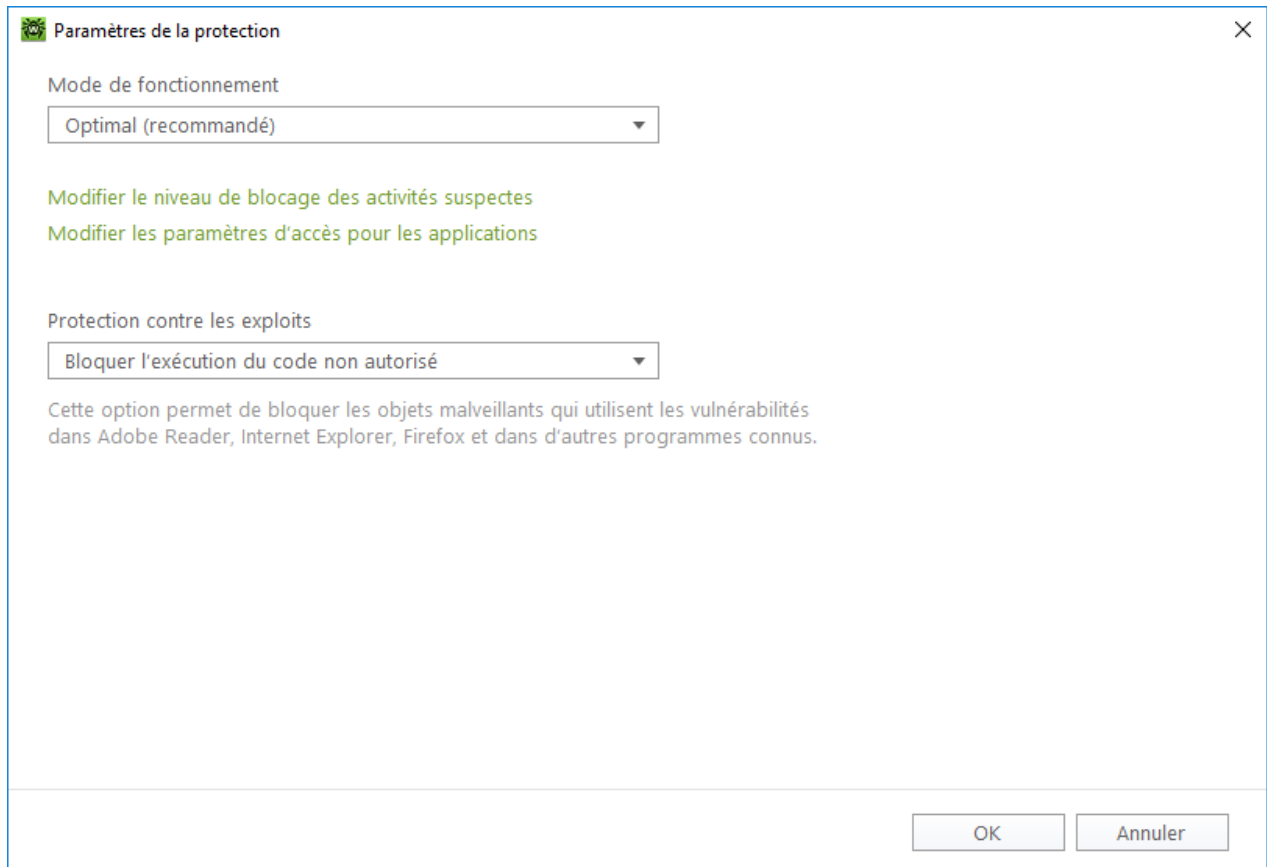


Figure 2. Paramètres de protection

Dans ce cas, vous pouvez spécifier le mode de protection à part pour les applications spécifiques 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 **Défini par l'utilisateur**. Dans cette fenêtre vous pouvez également créer un nouveau profil pour enregistrer les paramètres nécessaires.

Niveau de la protection préventive

Dans le mode **Optimal** 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. 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, 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 conflits de compatibilité avec des logiciels tiers 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 sur le téléchargement 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	Ce paramètre permet de détecter les processus qui pénètrent dans les applications en cours d'exécution ce qui représente une menace pour la sécurité de l'ordinateur.
Intégrité des fichiers des utilisateurs	Ce paramètre permet de détecter les processus qui modifient les fichiers utilisateur avec un algorithme connu qui indique que ce processus peut compromettre la sécurité de l'ordinateur.
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	Ce paramètre empêche les applications d'écrire sur les disques par secteurs en évitant le système de fichiers.
Téléchargement de pilotes	Ce paramètre empêche les applications de charger de nouveaux pilotes ou des pilotes inconnus.
Zones critiques Windows	<p>Les autres paramètres permettent de protéger les branches de registre 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



Objet protégé	Description
	<p>Autodémarrage de Windows :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadApplnit_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 <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\CurrentControlSet\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.



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.

9.2.7. Quarantaine

Cette fenêtre présente les données sur le contenu de la quarantaine qui sert à isoler les fichiers. 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.

Dans la partie centrale de la fenêtre, le tableau affiche les informations suivantes sur le statut de la quarantaine:

- **Objet** : nom de l'objet placé en quarantaine ;
- **Menace** : type du programme malveillant déterminé automatiquement 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 d'accès au fichier avant qu'il ne soit placé en quarantaine.

Gestion des objets en quarantaine

Les boutons suivants sont disponibles pour chaque objet :

- **Télécharger** : télécharger l'objet sélectionné du poste sur l'ordinateur de l'administrateur de réseau ;
- **Restaurer** : déplacer l'objet sélectionné vers le dossier d'origine sur le poste ;



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

- **Supprimer** : supprimer l'objet sélectionné de la quarantaine et du système ;
- **Vider la quarantaine** : supprimer tous les objets de la quarantaine.



10. Paramètres

Dans la rubrique de programme **Paramètres**, vous pouvez configurer les paramètres de Dr.Web KATANA Business Edition et les paramètres d'interaction de l'ordinateur d'administrateur et les postes sur lesquels Dr.Web KATANA a été installé. Les paramètres suivants sont accessibles :

- [la langue du logiciel](#) ;
- [la gestion des clés](#) ;
- [l'interaction réseau](#) ;
- [les paramètres d'accès au réseau](#) ;
- [la mise à jour de Dr.Web KATANA Business Edition](#).

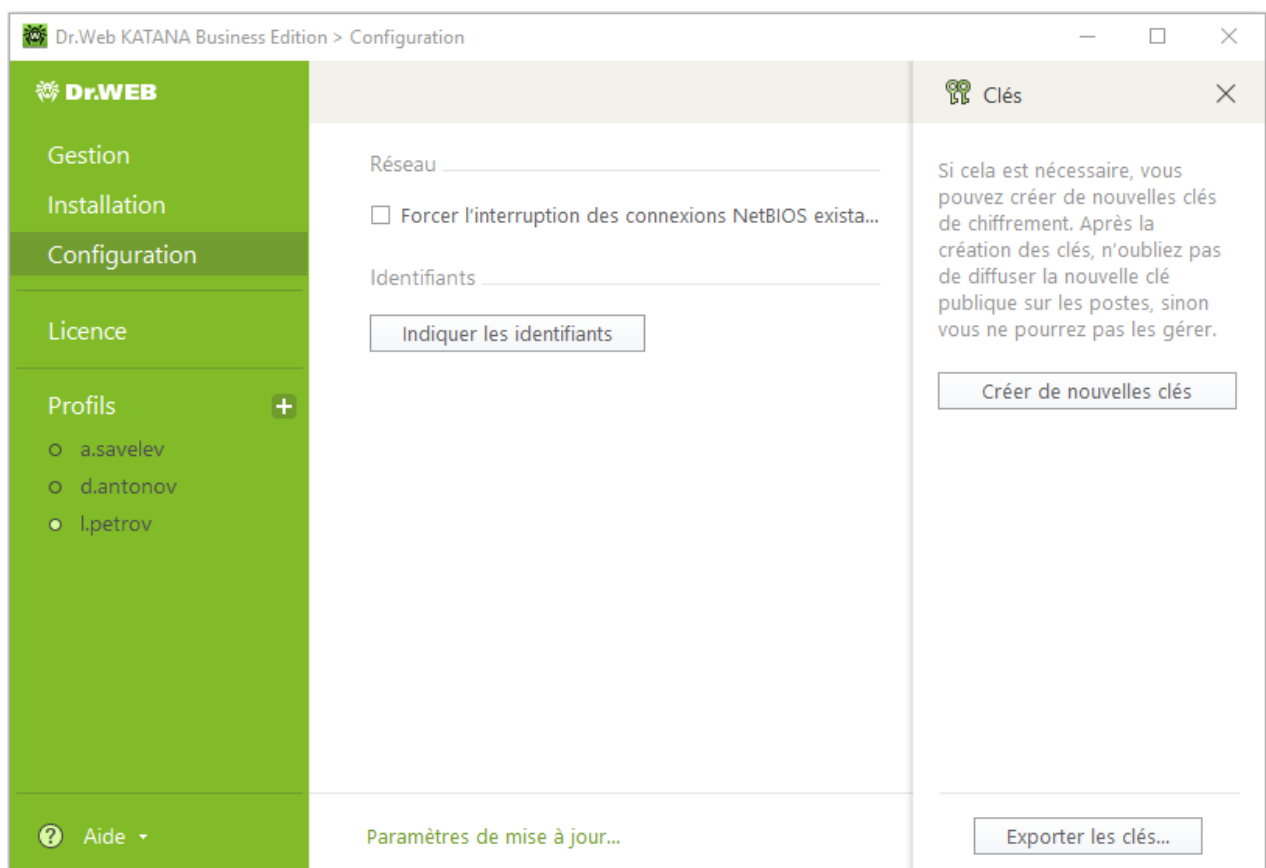



Figure 3. Configuration

Toutes les modifications de paramètres seront appliquées à la session actuelle. Vous pouvez les enregistrer dans le profil lors de la fermeture du programme ou lors du changement du profil.

Si vous rencontrez des difficultés lors de la configuration des paramètres de Dr.Web KATANA Business Edition, vous pouvez consulter l'Aide du logiciel en ouvrant la section **Aide**. Cette section se trouve dans la barre latérale du programme.



10.1. Langue du logiciel

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


10.2. Gestion des clés

Si cela est nécessaire, vous pouvez exporter les clés de chiffrement utilisées ou créer de nouvelles clés.


Pour créer de nouvelles clés

1. Dans la section **Paramètres** cliquez sur .
2. Dans la barre latérale qui s'ouvre, cliquez sur **Créer de nouvelles clés**.
3. Après la création de nouvelles clés distribuez-les sur les postes dans la section **Gestion**, en utilisant le panneau **Options**.



Vous ne pourrez pas continuer la gestion des postes jusqu'à ce que vous ne distribuiez une nouvelle clé publique. Pour ces postes, le statut  sera affiché dans la section **Gestion**.

Pour exporter les clés utilisées

1. Dans la section **Paramètres** cliquez sur .
2. Dans la barre latérale qui s'ouvre, cliquez sur **Exporter les clés**.
3. Sélectionnez le dossier dans lequel les clés de chiffrement seront enregistrées.

10.3. Paramètres de l'interaction réseau


Si nécessaire, vous pouvez configurer l'interaction réseau de l'ordinateur administrateur et des postes. Sélectionnez le mode **Forcer l'arrêt des connexions NetBIOS existantes**, pour interrompre toutes les connexions NetBIOS avec le poste avant l'installation, y compris les connexions au sein desquelles il y a des fichiers ouverts ou des tâches en exécution (cela est nécessaire pour la copie des fichiers et le lancement de Dr.Web KATANA).

10.4. Configuration des paramètres d'accès au réseau

Si vous n'avez pas de droits pour accéder au réseau, avant d'ajouter les postes vous verrez une notification correspondante dans la rubrique **Installation**. Pour installer Dr.Web KATANA avec succès, entrez le nom d'utilisateur et le mot de passe en cliquant sur le bouton **Spécifier les**



identifiants dans la section **Paramètres**. Vous pouvez également créer un nouveau compte ou supprimer le compte existant.


- Pour créer un nouveau compte, entrez le nom d'utilisateur et le mot de passe. Cliquez sur le bouton **Ajouter**. Le compte créé va apparaître dans la liste.
- Pour supprimer un compte existant, placez le curseur sur son nom dans la liste et cliquez sur .

Notez que l'administrateur ne peut pas voir les mots de passe des comptes.

10.5. Mise à jour de Dr.Web KATANA Business Edition

Pour modifier les paramètres de la mise à jour de Dr.Web KATANA Business Edition, ouvrez la rubrique **Paramètres** et cliquez sur le lien **Paramètres de la mise à jour**.

Mise à jour automatique du programme

Si l'option **Vérifier les mises à jour automatiquement** est activée, Dr.Web KATANA Business Edition vérifie la disponibilité des mises à jour et les télécharge. Dans ce cas, l'icône  apparaît dans le menu latéral à côté du nom de la rubrique **Aide**. Pour une mise à jour complète, redémarrez Dr.Web KATANA Business Edition. Pour ce faire, procédez comme suit :

1. Dans le menu déroulant de la section **Aide**, sélectionnez l'élément **A propos de**.
2. Dans la fenêtre qui s'affiche, cliquez sur le bouton **Redémarrer pour mettre à jour**.

Mise à jour manuelle du programme

Si l'option **Vérifier les mises à jour automatiquement** est désactivée sur votre ordinateur, Dr.Web KATANA Business Edition est mis à jour manuellement. Pour mettre à jour le logiciel, procédez comme suit :

1. Dans le menu déroulant de la section **Aide**, cliquez sur l'élément **A propos de**, puis sur le bouton **Vérifier les mises à jour**. Si les mises à jour sont disponibles, le téléchargement commence.
2. Pour une mise à jour complète de Dr.Web KATANA Business Edition, redémarrez le programme. Pour ce faire, procédez comme suit :
 - a) Dans le menu déroulant de la section **Aide**, sélectionnez l'élément **A propos de**.
 - b) Dans la fenêtre qui s'affiche, cliquez sur le bouton **Redémarrer pour mettre à jour**.



Paramètres de la mise à jour

Si cela est nécessaire, vous pouvez sélectionner les modes suivants de la mise à jour de Dr.Web KATANA Business Edition :

- **Utiliser les connexions HTTPS** : activez cette option si vous voulez télécharger les mises à jour via le protocole sécurisé ;
- **Utiliser un serveur proxy** : activez cette option si vous voulez utiliser le serveur proxy et spécifiez les paramètres de connexion à ce serveur :

Paramètre	Description
Adresse	Spécifiez l'adresse du serveur proxy.
Port	Spécifiez le port du serveur proxy.
Nom d'utilisateur	Spécifiez le nom du compte pour la connexion au serveur proxy.
Mot de passe	Spécifiez le mot de passe du compte utilisé pour la connexion au serveur proxy.
Type d'authentification	Sélectionnez le type d'authentification nécessaire pour la connexion au serveur proxy.



11. Gestion des licences

Dans la rubrique de programme **Licence** s'affichent les informations sur la licence disponible de Dr.Web KATANA Business Edition.

Dans certains cas, par exemple, si la licence expire ou que vous voulez augmenter le nombre de postes pour l'installation de Dr.Web KATANA, vous pouvez décider d'acheter une nouvelle licence Dr.Web. Dans cette rubrique, vous pouvez remplacer une licence par une autre.

Pour changer de licence

1. Cliquez sur le bouton **Remplacer la licence**.
2. Dans la fenêtre qui s'ouvre, spécifiez le chemin d'accès au nouveau fichier clé.



Après l'ajout de la nouvelle licence, elle sera automatiquement distribuée sur les postes sur lesquels Dr.Web KATANA est installé. Vous n'avez pas besoin de réinstaller ni d'arrêter Dr.Web KATANA Business Edition et Dr.Web KATANA sur les postes.

Le lien [Mon Dr.Web](#) ouvre votre espace personnel sur le site officiel de Doctor Web. Cette page vous fournit les 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.



12. Annexe A. Méthodes de détection

Dr.Web KATANA utilise des technologies de blocage des processus malveillants basées sur l'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'activité 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 d'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 de programmes de Troie sous forme d'un nouveau dispositif virtuel ;
- il ne permet pas au logiciel malveillant de perturber le fonctionnement normal des services système.



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.

Système cloud de la mise à jour des algorithmes de blocage Dr.Web ShellGuard

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 collectés :

- 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 populaires ;
- les informations sur les signatures numériques des logiciels publicitaires ou potentiellement dangereux ;
- les algorithmes de protection de telles ou telles applications.

