Dr.WEB

Enterprise Security Suite

Guide sur le déploiement du réseau antivirus

Dr.Web Enterprise Security Suite
Version 11.0.2
Guide sur le déploiement du réseau antivirus
31/07/2020

Doctor Web, Siège social en Russie

Adresse : 2-12A, 3e rue Yamskogo polya, 125040 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

Chapitre 1. Dr.Web Enterprise Security Suite

1.1. Introduction

1.1.1. Destination du document

L'instruction sur le déploiement du réseau antivirus contient de brèves informations sur l'installation et la configuration initiale des composants du réseau antivirus. Pour des informations détaillées, consultez la documentation d'administrateur.

La documentation de l'administrateur du réseau antivirus contient les parties suivantes :

1. **Manuel d'installation**
2. **Manuel Administrateur**
3. **Annexes**

De plus, les Manuels suivants sont fournis :

1. **Manuels de gestion des postes**
2. **Manuels Utilisateur**

Tous les Manuels listés sont fournis au sein du produit Dr.Web Enterprise Security Suite et vous pouvez les ouvrir via le Centre de gestion de la sécurité Dr.Web.

Avant de prendre connaissance de ces documents, merci de vous assurer que vous lisez la dernière version des Manuels correspondant à votre version de produit. Les manuels sont constamment mis à jour, et leur dernière version est disponible sur le site officiel de Doctor Web à l'adresse https://download.drweb.com/doc/.

1.1.2. Légende

Conventions

Les styles de texte utilisées dans ce manuel :

Styles	Utilisés
	Notice/indication importante.
	Avertissement sur des situations potentielles d'erreurs et sur les éléments importants auxquels il faut faire attention.
Réseau antivirus	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.

Abréviations

Les abréviations suivantes peuvent être utilisées dans le Manuel :

- ACL : listes de contrôle d'accès (Access Control List),
- CDN : réseau de distribution de contenu (Content Delivery Network),
- DFS : système de fichiers distribués (Distributed File System),
- DNS : système de noms de domaine (Domain Name System),
- FQDN : nom de domaine complètement qualifié (Fully Qualified Domain Name),
- GUI : interface graphique utilisateur (Graphical User Interface), une version GUI du logiciel est une version utilisant des outils GUI,
- MTU : taille maximale de l'unité de transmission (Maximum Transmission Unit),
- NAP : Protection d'accès réseau (Network Access Protection),
- TTL : durée de Vie (Time To Live),
- UDS : socket du domaine UNIX (UNIX Domain socket),
- BD, SGBD : base de données, système de gestion de base de données,

- SGM Dr.Web : Système Global de Mises à jour Dr.Web,
- LAN : réseau local,
- OS : système d'exploitation.

1.2. A propos du produit

Dr.Web Enterprise Security Suite est conçu pour la mise en oeuvre et la gestion d'une protection antivirus fiable non seulement du réseau interne de l'entreprise, y compris des appareils mobiles mais aussi des ordinateurs de maison des employés.

Un ensemble d'ordinateurs et d'appareils mobiles sur lesquels les composants interagissants de Dr.Web Enterprise Security Suite sont installés représente un *réseau antivirus*.

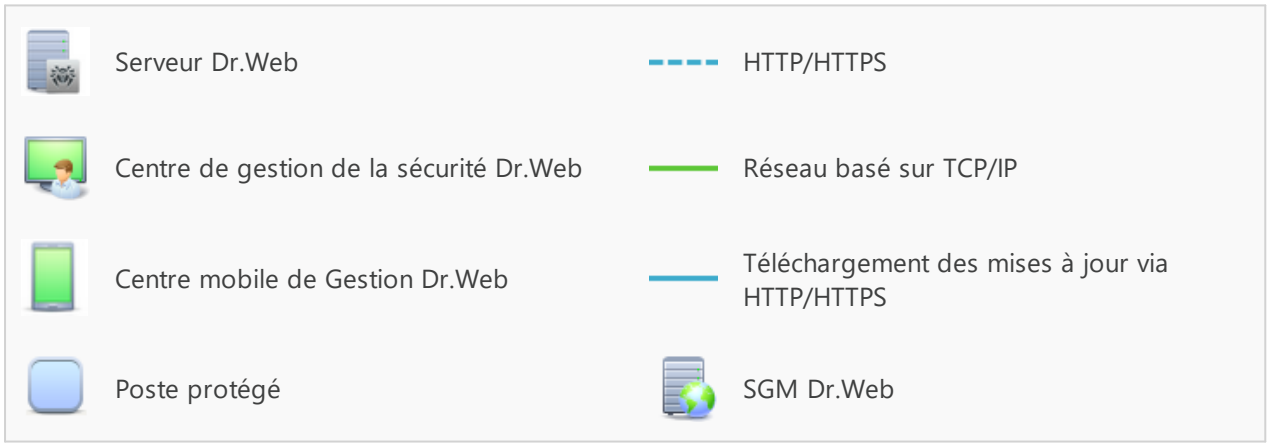

Figure 1-1. Structure logique du réseau antivirus

Le réseau antivirus Dr.Web Enterprise Security Suite repose sur une structure *client-serveur*. Ses composants sont installés sur les postes et les appareils mobiles des utilisateurs et des

administrateurs ainsi que sur les postes dotés des fonctionnalités de Serveurs LAN. Ces composants échangent des informations via les protocoles réseau TCP/IP. Vous pouvez installer (et plus tard gérer) le logiciel antivirus sur les postes protégés via LAN ou via Internet.

Serveur de protection centralisée

Le Serveur de protection centralisée peut être installé sur n'importe quel ordinateur du réseau antivirus et pas uniquement sur le poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le paragraphe Pré-requis système.

Le logiciel du serveur est indépendant de la plateforme et permet d'utiliser en tant que Serveur un ordinateur tournant sous les systèmes d'exploitation suivants :

- Windows®,
- OS de la famille UNIX® (Linux®, FreeBSD®).

Le Serveur de protection centralisée conserve les distributions des packages antivirus appropriés aux différents OS installés sur les postes protégés, les mises à jour des bases virales ainsi que celles des packages antivirus, les clés utilisateurs et les configurations des packages pour les postes protégés. Le Serveur reçoit des mises à jour de composants de protection antivirus et des bases virales via Internet depuis les serveurs du Système Global de Mise à jour et distribue les mises à jour sur les postes protégés.

Base de données commune

La base de données commune se connecte au Serveur de protection centralisée et contient les statistiques des événements du réseau antivirus, les paramètres du Serveur, les paramètres des postes protégés et des composants antivirus installés sur les postes protégés.

Centre de gestion de la protection centralisée

Le Centre de gestion de la protection centralisée s'installe automatiquement avec le Serveur et fournit l'interface web permettant la gestion à distance du Serveur et du réseau antivirus par le biais de la modification des configurations du Serveur et des postes protégés conservées sur le Serveur et sur les postes.

Le Centre de gestion peut être ouvert sur n'importe quel ordinateur ayant l'accès au Serveur. Le Centre de gestion peut être utilisé sus n'importe quel système d'exploitation avec la fonctionnalité complète sous les navigateurs web suivants :

- Windows® Internet Explorer®,
- Microsoft Edge®,
- Mozilla® Firefox®,
- Google Chrome®.

Vous pouvez consulter la liste des options d'utilisation possibles dans le p. Pré-requis système.

Le Serveur web est automatiquement installé avec le Serveur et représente une partie du Centre de gestion de la sécurité Dr.Web. La tâche principale du Serveur web est d'interagir avec les pages web du Centre de gestion et les connexions réseau des clients.

Centre de gestion Mobile de la protection centralisée

Le Centre de gestion Mobile est fourni en tant que composant à part destiné à installer et lancer le logiciel sur les appareils mobiles tournant sous iOS® et OS Android™. Les exigences générales pour l'application sont mentionnées dans le p. Pré-requis système.

La connexion du Centre de gestion Mobile au Serveur est effectuée à la base des identifiants de l'administrateur du réseau antivirus, y compris via le protocole crypté.

Vous pouvez télécharger le Centre de gestion Mobile depuis le Centre de gestion ou directement sur App Store ou Google Play.

Protection des postes du réseau

Sur les postes et les appareils mobiles du réseau s'effectue l'installation du module gérant (l'Agent) et du package antivirus pour le système d'exploitation correspondant.

Le logiciel du serveur est indépendant de la plateforme et permet de protéger des ordinateurs et des appareils mobiles tournant sous les système d'exploitation suivants :

- Windows®,
- OS de la famille UNIX®,
- macOS®,
- OS Android.

Les ordinateurs personnels et les serveurs LAN peuvent être considérés comme postes protégés. Notamment, la protection antivirus du système de courrier Microsoft® Outlook® est supportée.

Le module gérant effectue des mises à jour régulières des composants antivirus et des bases virales depuis le Serveur et envoie sur le Serveur des informations sur les événements du poste protégé.

En cas d'indisponibilité du Serveur de protection centralisée la mise à jour de bases virales de postes protégés est effectuée directement depuis le Système Global de Mise à jour via Internet.

Assurance de la connexion entre les composants du réseau antivirus

Pour assurer la connexion stable et sécurisée entre les composants du réseau antivirus, les fonctionnalités suivantes sont fournies :

Serveur proxy Dr.Web

Le Serveur proxy peut être optionnellement inclus dans le réseau antivirus. L'objectif principal du Serveur proxy consiste à assurer la connexion entre le Serveur et les postes protégés dans le cas où l'accès direct de l'organisation deviendrait impossible.

Compression du trafic

Lors de la transmission de données entre les composants du réseau antivirus, les algorithmes spéciaux de compression sont utilisés, ce qui assure le trafic réseau minimum.

Chiffrement du trafic

Lors de la transmission de données entre les composants du réseau antivirus, le chiffrement est utilisé ce qui assure la protection supplémentaire.

Options supplémentaires

NAP Validator

NAP Validator est fourni en tant que composant supplémentaire qui permet d'utiliser la technologie Microsoft Network Access Protection (NAP) pour vérifier le fonctionnement du logiciel sur les postes protégés.

Chargeur du Référentiel

Chargeur du Référentiel Dr.Web est fourni en tant qu'utilitaire supplémentaire qui permet de télécharger les produits Dr.Web Enterprise Security Suite depuis le Système global de mises à jour. Il peut être utilisé pour télécharger les mises à jour de produits Dr.Web Enterprise Security Suite pour placer les mises à jour sur le Serveur qui n'est pas connecté à Internet.

1.3. Pré-requis système

Le fonctionnement du Serveur Dr.Web requiert :

Composant	Pré-requis
CPU	CPU supportant les instructions SSE2 et ayant la fréquence d'horloge de 1,3 Ghz ou supérieure.

Composant	Pré-requis
Mémoire vive	• Pré-requis minimum : 1 Go. • Pré-requis recommandés : 2 Go et plus.
Espace disque	Pas moins de 12 Go : jusqu'à 8 Go pour une base de données embarquée (répertoire d'installation) et jusqu'à 4 Go dans le répertoire système temporaire (pour le fonctionnement des fichiers).
Système d'exploitation	• Windows ; • Linux ; • FreeBSD. La liste complète des OS supportés est fournie dans les **Annexes**, dans l'Annexe A.
Support des environnements virtuels et cloud	Le fonctionnement est supporté sous les systèmes d'exploitation qui satisfont les pré-requis ci-dessus, dans les environnements virtuels et cloud, y compris : • VMware ; • Hyper-V ; • Xen ; • KVM.

Les utilitaires supplémentaires fournis avec le Serveur Dr.Web (disponibles pour le téléchargement via le Centre de gestion, section **Administration** → **Utilitaires**) doivent être lancés sur l'ordinateur qui satisfait les pré-requis système du Serveur Dr.Web.

Le Centre de gestion de la sécurité Dr.Web requiert :

a) Navigateur :

Navigateur	Support
Windows Internet Explorer 11	Supporté.
Microsoft Edge 0.10 ou supérieur	
Mozilla Firefox 25 et supérieur	
Google Chrome 30 et supérieur	
Opera® 10 et supérieur	Vous pouvez les utiliser mais le fonctionnement sous ces navigateurs web n'est pas garanti.
Safari® 4 et supérieur	

b) La résolution d'écran recommandée pour utiliser le Centre de gestion est 1280x1024 pt.

Le Centre de gestion Mobile Dr.Web requiert :

Les pré-requis varient en fonction du système d'exploitation sur lequel l'application est installée :

Système d'exploitation	Pré-requis	
	Version du système d'exploitation	**Appareil**
iOS	iOS 8 ou supérieur	Apple® iPhone® Apple® iPad®
Android	Android 4.0 et supérieur	–

Le fonctionnement de l'Agent Dr.Web et du package antivirus complet requiert :

Les pré-requis varient en fonction du système d'exploitation sur lequel l'application est installée (voir la liste complète des OS supportés dans les **Annexes**, l'Annexe A. Liste complète des OS supportés) :

- OS Windows :

Composant	Pré-requis
CPU	CPU ayant la fréquence d'horloge de 1 Ghz et plus.
Mémoire vive libre	Au moins 512 Mo.
Espace disque libre	Pas moins de 1 Go pour les fichiers exécutables + espace disque supplémentaire pour les journaux et les fichiers temporaires.

- OS de la famille Linux :

Composant	Pré-requis
CPU	Processeurs supportés avec architecture et système de commandes Intel/AMD : 32 bits (IA-32, x86) ; 64 bits (x86-64, x64, amd64).
Mémoire vive libre	Au moins 512 Mo.
Espace disque libre	Au moins de 400 Mo d'espace disque libre sur le volume qui contient les répertoires de l'Antivirus.

- macOS, OS Android : les pré-requis pour la configuration correspondent aux pré-requis pour le système d'exploitation.

Le fonctionnement de l'Agent Dr.Web est supporté sous les systèmes d'exploitation qui satisfont aux pré-requis ci-dessus, dans les environnements virtuels et cloud, y compris :

- VMware ;
- Hyper-V ;
- Xen ;
- KVM.

1.4. Kit de distribution

La distribution Dr.Web Enterprise Security Suite est fournie en fonction de OS du Serveur Dr.Web sélectionné :

1. Pour les OS de la famille UNIX :
   - `drweb-11.00.2-<assemblage>-esuite-server-<version_de_l'OS>.tar.gz.run`
     Distribution principale du Serveur Dr.Web*
   - `drweb-11.00.2-<assemblage>-esuite-extra-<version_de_l'OS>.tar.gz.run`
     Distribution supplémentaire du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-proxy-<version_de_l'OS>.tar.gz.run`
     Serveur proxy Dr.Web
   - `drweb-reploader-<OS>-<nombre de bits>`
     Version de console du Chargeur du référentiel Dr.Web
2. Sous Windows :
   - `drweb-11.00.2-<assemblage>-esuite-server-<version_de_l'OS>.exe`
     Distribution principale du Serveur Dr.Web*
   - `drweb-11.00.2-<assemblage>-esuite-extra-<version_de_l'OS>.exe`
     Distribution supplémentaire du Serveur Dr.Web
   - `drweb-11.00.2-<assemblage>-esuite-proxy-<version_de_l'OS>.exe`
     Serveur proxy Dr.Web
   - `drweb-11.05.4-<assemblage>-esuite-agent-activedirectory.msi`
     Agent Dr.Web pour Active Directory
   - `drweb-11.00.1-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe`
     Utilitaire de la modification du schéma Active Directory
   - `drweb-11.00.1-<assemblage>-esuite-aduac-<version_de_l'OS>.msi`
     Utilitaire de la modification des attributs des objets Active Directory
   - `drweb-11.00.1-<assemblage>-esuite-napshv-<version_de_l'OS>.msi`
     NAP Validator

- `drweb-11.05.2-<assemblage>-esuite-agent-full-windows.exe`

  Installateur complet de l'Agent Dr.Web. Inclus dans la distribution supplémentaire du Serveur Dr.Web.

- `drweb-reploader-windows-<nombre_de_bits>.exe`

  Version de console du Chargeur du référentiel Dr.Web

- `drweb-reploader-gui-windows-<nombre_de_bits>.exe`

  Version graphique du Chargeur du référentiel Dr.Web

***La distribution principale du Serveur Dr.Web contient les composants suivants :**

- logiciel du Serveur Dr.Web pour l'OS correspondant,
- logiciel des Agents Dr.Web et des packages antivirus pour les postes sous OS Windows,
- logiciel du Centre de gestion de la sécurité Dr.Web,
- bases virales,
- Extension pour le Centre de gestion de la sécurité Dr.Web,
- Extension Dr.Web Server FrontDoor,
- documentation, modèles, exemples.

Outre la distribution, les numéros de série seront également fournis. Après les avoir enregistrés, vous recevrez les fichiers contenant les clés.

Chapitre 2. Création d'un réseau antivirus

Brève instruction de déploiement d'un réseau antivirus :

1. Rédigez un plan de la structure du réseau antivirus. Le plan doit comprendre tous les postes et les appareils mobiles à protéger.

   Sélectionnez l'ordinateur qui va accomplir les fonctions du Serveur Dr.Web. Le réseau antivirus peut comprendre plusieurs Serveurs Dr.Web. Les particularités d'une telle configuration sont décrites dans le **Manuel Administrateur**, le p. Particularités du réseau avec plusieurs Serveurs Dr.Web.

   Le Serveur Dr.Web peut être installé sur n'importe quel ordinateur et pas uniquement sur la poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le paragraphe Pré-requis système.

   La même version de l'Agent Dr.Web est installée sur tous les postes protégés, y compris les serveurs LAN. La différence consiste en la liste des composants antivirus installés spécifiée par les paramètres sur le Serveur.

   Pour installer le Serveur Dr.Web et l'Agent Dr.Web une procédure d'accès unitaire aux ordinateurs respectifs sera requise (accès physique ou via des outils de gestion à distance permettant de lancer et de contrôler les programmes). Toutes les opérations ultérieures seront effectuées depuis le poste de l'administrateur du réseau antivirus (voire de l'extérieur du réseau local) et ne nécessitent aucun accès aux Serveurs Dr.Web ni aux postes de travail.

   Quand vous planifiez un réseau antivirus, pensez à créer une liste des personnes qui doivent avoir accès au Centre de gestion en fonction de leurs responsabilités. Préparez, également, une liste de rôles avec les responsabilités associées à chaque rôle. Il faut créer un groupe administratif pour chaque rôle. Pour associer les administrateurs aux rôles, placez les comptes d'administrateurs dans les groupes administratifs. Si nécessaire, vous pouvez hiérarchiser les groupes (rôles) dans un système à plusieurs niveaux et configurer les droits d'accès administratifs pour chaque niveau séparément.

   Pour en savoir plus sur la gestion des groupes administratifs et des règles d'accès, consultez le **Manuel d'installation**, la Chapitre 5 : Administrateurs du réseau antivirus

2. Déterminez les produits à installer sur les noeuds du réseau en fonction du plan rédigé. Pour en savoir plus sur les produits fournis, consultez la rubrique Kit de distribution.

   Vous pouvez acheter tous les produits nécessaires en boîte Dr.Web Enterprise Security Suite ou les télécharger sur les site de Doctor Web https://download.drweb.com/.

   Les Agents Dr.Web pour le poste sous OS Android, OS Linux, macOS peuvent également être installés depuis les packages pour les produits autonomes et connectés plus tard au Serveur centralisé Dr.Web. Vous pouvez consulter la description des paramètres des Agents dans les **Manuels utilisateur** correspondants.

3. Installez la distribution principale du Serveur Dr.Web sur un ou plusieurs ordinateurs. L'installation est décrite dans le **Manuel d'installation**, le p. Installation du Serveur Dr.Web.

   Le Centre de gestion de la sécurité Dr.Web est installé avec le Serveur.

   Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.

4. Si le réseau antivirus inclut les postes protégés sous OS Android, OS Linux, macOS, installez la distribution supplémentaire du Serveur Dr.Web sur tous les ordinateurs sur lesquels la distribution principale du Serveur est installée.
5. Si nécessaire, installez et configurez le Serveur proxy. Vous pouvez consulter la description dans le **Manuel d'installation**, le p. Installation du Serveur proxy.
6. Pour configurer le Serveur et le logiciel antivirus sur les postes, il faut se connecter au Serveur depuis le Centre de gestion de la sécurité Dr.Web.

   

   Le Centre de gestion peut être ouvert sur n'importe quel ordinateur et pas uniquement sur celui sur lequel est installé le Serveur. Une connexion réseau doit être établie avec l'ordinateur sur lequel le Serveur est installé.

   Le Centre de gestion est accessible à l'adresse suivante :

   `http://<adresse_du_Serveur>:9080`

   ou

   `https://<adresse_du_Serveur>:9081`

   où comme valeur *<adresse_du_Serveur>* spécifiez l'adresse IP ou le nom de domaine de l'ordinateur sur lequel est installé le Serveur Dr.Web.

   Dans la boîte de dialogue d'authentification, entrez le nom et le mot de passe administrateur. Par défaut, les identifiants de l'administrateur ayant tous les droits sont :

   - Nom – **admin**.
   - Mot de passe :
     - sous Windows – le mot de passe a été spécifié lors de l'installation du Serveur.
     - pour les OS de la famille UNIX – mot de passe qui a été automatiquement créé au cours de l'installation du Serveur (voir aussi le **Manuel d'installation**, le p. Installation du Serveur Dr.Web pour les OS de la famille UNIX®).

   Si la connexion au Serveur est établie, la fenêtre principale du Centre de gestion va s'ouvrir (pour en savoir plus, consultez le **Manuel Administrateur**, le p. Centre de gestion de la sécurité Dr.Web).
7. Effectuez la configuration initiale du Serveur (vous pouvez consulter le description détaillée des paramètres du Serveur dans le **Manuel administrateur**, dans la Chapitre 8 : Configuration du Serveur Dr.Web) :
   a. Dans la rubrique Gestionnaire de licences, ajoutez une ou plusieurs clés de licence et diffusez-les sur les groupes correspondants, notamment sur le groupe **Everyone**. Cette

étape est obligatoire si la clé de licence n'a pas été spécifiée lors de l'installation du Serveur.

b. Dans la rubrique Configuration générale du référentiel, spécifiez les composant du réseau antivirus à mettre à jour depuis le SGM Dr.Web. Dans la rubrique Statut du référentiel effectuez la mise à jour des produits du référentiel du Serveur. La mise à jour peut prendre un long temps. Attendez la fin de la mise à jour avant de continuer la configuration.

c. Vous trouverez les informations sur la version du Serveur sur la page **Administration** → **Serveur Dr.Web**. Si la nouvelle version est disponible, mettez à jour le Serveur. La procédure est décrite dans le **Manuel Administrateur**, dans le p. Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde.

d. Si nécessaire, configurez les Connexions réseau pour modifier les paramètres réseau spécifiés par défaut et utilisés pour l'interaction de tous les composants du réseau antivirus.

e. Si nécessaire, configurez la liste d'administrateurs du Serveur. L'authentification externe des administrateurs est également possible. Pour en savoir plus, consultez le **Manuel administrateur**, la Chapitre 5 : Administrateurs du réseau antivirus.

f. Avant d'utiliser l'antivirus, il est recommandé de modifier la configuration du répertoire de sauvegarde des données critiques du Serveur (voir le **Manuel Administrateur**, le p. Configuration de la planification du Serveur Dr.Web). Il est préférable de placer ce répertoire sur un autre disque local afin de minimiser la probabilité de perte simultanée des fichiers du logiciel Serveur et de ceux de la copie de sauvegarde.

8. Spécifiez les paramètres et la configuration du logiciel antivirus pour les postes de travail (vous pouvez consulter la description détaillée de la configuration de groupes et de postes dans le **Manuel administrateur**, la Chapitre 6 et la Chapitre 7) :

   a. Si nécessaire, créez les groupes utilisateur de postes.

   b. Spécifiez les paramètres du groupe **Everyone** et des groupes utilisateur crées. Notamment configurez la rubrique des composants à installer.

9. Installez le logiciel de l'Agent Dr.Web sur les postes de travail.

   Dans la rubrique Fichiers d'installation, consultez la liste des fichiers fournis pour l'installation de l'Agent. Sélectionnez le type d'installation en fonction du système d'exploitation du poste, la possibilité de l'installation à distance, la configuration du Serveur lors de l'installation de l'Agent, etc. Par exemple :

   - Sil les utilisateurs installent l'antivirus eux-mêmes, utilisez les packages d'installation personnels qui sont créés via le Centre de gestion séparément pour chaque poste. Vous pouvez envoyer aux utilisateurs des e-mails avec ce type de package directement du Centre de gestion. Après l'installation, les postes se connectent automatiquement au Serveur.
   - S'il est nécessaire d'installer l'antivirus sur plusieurs postes d'un seul groupe utilisateur, vous pouvez utiliser le package d'installation de groupe créé en un seul exemplaire via le Centre de gestion pour plusieurs postes d'un groupe spécifique.

- Utilisez l'installateur réseau pour l'installation à distance sur un ou plusieurs postes en même temps (uniquement pour les postes tournant sous Windows). L'installation s'effectue via le Centre de gestion.
- Il est également possible d'installer l'antivirus à distance par réseau à l'aide du service Active Directory sur un ou plusieurs postes en même temps. Pour ce faire, il faut utiliser l'installateur de l'Agent Dr.Web pour les réseaux Active Directory fourni avec la distribution Dr.Web Enterprise Security Suite, mais séparément de l'installateur du Serveur.
- Si, lors de l'installation, il faut diminuer la charge sur le canal de communication entre le Serveur et les postes, vous pouvez utiliser l'installateur complet qui effectue l'installation de l'Agent et des composants de protection en même temps.
- Installation sur les postes sous OS Android, OS Linux et macOS peut s'effectuer de manière locale conformément aux règles générales. Le produit autonome installé peut se connecter au Serveur conformément à la configuration correspondante.

Pour obtenir les installateurs sous les OS autres que Windows et pour installer la distribution complète, l'installation de la distribution supplémentaire (extra) du Serveur Dr.Web est requise.

Pour un fonctionnement correct de l'Agent Dr.Web sur l'OS de serveur Windows à partir de Windows Server 2016, il faut désactiver Windows Defender manuellement en utilisant les politiques de groupe.

10. Une fois installés sur les postes, les Agents se connectent automatiquement au Serveur. L'approbation des postes antivirus sur le Serveur est effectuée selon la politique que vous sélectionnez (les paramètres sont décrits dans le **Manuel Administrateur**, le p. Politique de connexion des postes) :
    a. En cas d'installation depuis les packages d'installation et la configuration de l'approbation automatique sur le Serveur, les postes de travail sont enregistrés automatiquement à la première connexion au Serveur et l'approbation supplémentaire n'est pas requise.
    b. En cas d'installation depuis les installateurs et la configuration de l'approbation manuelle, l'administrateur doit approuver manuellement de nouveaux postes pour les enregistrer sur le Serveur. Dans ce cas, les nouveaux postes ne se connectent pas automatiquement, mais ils sont déplacés par le Serveur dans le groupe de novices.
11. Après la connexion au Serveur et l'obtention des paramètres, l'ensemble des composants du package antivirus est installé sur le poste. Cet ensemble est spécifié dans les paramètres du groupe primaire du poste.

Pour terminer l'installation des composants sur le poste, le redémarrage de l'ordinateur est requis.

12. La configuration des postes et du logiciel est également possible après l'installation (vous pouvez consulter la description détaillée dans le **Manuel administrateur**, dans la Chapitre 7).

Annexe A. Licence

Le fonctionnement de la solution antivirus Dr.Web Enterprise Security Suite nécessite une licence.

Le contenu et le prix de la licence pour l'utilisation de Dr.Web Enterprise Security Suite dépendent du nombre de postes protégés y compris les serveurs inclus dans le réseau Dr.Web Enterprise Security Suite et qui tournent comme postes protégés.

Signalez cette information au vendeur de licence au moment de l'achat de Enterprise Security Suite Dr.Web. Le nombre de Serveurs Dr.Web utilisés n'influence pas le prix de la licence.

Fichier clé de licence

Les droits de l'utilisateur relatifs à l'utilisation de Dr.Web Enterprise Security Suite sont déterminés par les fichiers clés de licence.

Le format de fichier clé est protégé contre l'édition avec un mécanisme de signature numérique. Toute modification de ce fichier le rend invalide. Afin d'éviter tout endommagement involontaire du fichier clé, il ne faut pas le modifier ni l'enregistrer à la fermeture de l'éditeur de texte.

Les fichiers clés de licence sont fournis sous forme d'une archive zip contenant un ou plusieurs fichiers clés pour les postes à protéger.

L'utilisateur peut obtenir les fichiers clés de licence par l'un des moyens suivants :

- Le fichier clé de licence est inclus dans le package de l'antivirus Dr.Web Enterprise Security Suite au moment de l'achat, s'il a été inclus dans la distribution. Mais d'habitude seuls les numéros de série sont fournis.
- Le fichier clé de licence est envoyé aux utilisateurs par e-mail après l'enregistrement du numéro de série sur le site web de Doctor Web (https://products.drweb.com/register/, sauf indication contraire spécifiée dans la carte d'enregistrement du produit). Veuillez visiter le site indiqué pour remplir un formulaire où vous devez spécifier quelques informations personnelles et saisir dans le champ approprié le numéro de série (vous le trouverez sur la carte produit). Une archive contenant vos fichiers clés vous sera envoyée à l'adresse que vous avez spécifiée. Vous pourrez également télécharger les fichiers clés directement sur le site mentionné ci-dessus.
- Le fichier clé de licence peut être fourni sur un support à part.

Il est recommandé de conserver le fichier clé de licence pendant la durée de validité de la licence. Vous pouvez l'utiliser en cas de réinstallation ou restauration des composants de l'antivirus. En cas de perte du fichier clé de licence, vous pouvez repasser la procédure

d'enregistrement sur le site et obtenir le fichier clé de licence de nouveau. Dans ce cas, il est nécessaire de spécifier le même numéro de série et les mêmes informations sur l'utilisateur que vous avez soumis lors du premier enregistrement ; seule l'adresse e-mail peut être modifiée. Si c'est le cas, le fichier clé sera envoyé à la nouvelle adresse e-mail.

Pour tester l'Antivirus, vous pouvez utiliser des fichiers clé de démonstration. Les fichiers clés de démo fournissent les fonctionnalités complètes des composants antivirus, mais leur durée de validité est limitée. Pour obtenir des fichiers clés de démo, vous devez remplir un formulaire qui se trouve sur la page suivante https://download.drweb.com/demoreq/biz/. Votre demande sera traitée à titre individuel. En cas de réponse positive, une archive contenant les fichiers clés vous sera envoyée à l'adresse spécifiée.

Pour en savoir plus sur les principes et les particularités de la licence Dr.Web Enterprise Security Suite, consultez le **Manuel Administrateur**, les sous-rubriques Chapitre 2. Licence.

L'utilisation des fichiers clés de licence lors de l'installation du programme est décrite dans le **Manuel d'installation**, p. Installer le Serveur Dr.Web.

L'utilisation des fichiers clés de licence pour un réseau antivirus déjà déployé est décrite en détails dans le **Manuel Administrateur**, p. Gestionnaire de licences.

Annexe B. Support technique

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

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

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

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

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