



Dr.WEB

Enterprise Security Suite

Guide sur le déploiement du réseau antivirus



© **Doctor Web, 2024. 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 Enterprise Security Suite
Version 13.0
Guide sur le déploiement du réseau antivirus
07/03/2024

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

Chapitre 1 : Introduction	5
1.1. Destination du document	5
1.2. Légende	5
Chapitre 2 : Dr.Web Enterprise Security Suite	7
2.1. A propos du produit	7
2.2. Pré-requis système	11
2.3. Kit de distribution	22
Chapitre 3 : Création d'un réseau antivirus	25
Annexe A. Octroi de licence	30
Annexe B. Support technique	32



Chapitre 1 : Introduction

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**
3. **Manuels sur Web API**
4. **Manuel sur la base de données du Serveur Dr.Web**

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, leur dernière version est disponible sur le site officiel de Doctor Web à l'adresse <https://download.drweb.com/doc>.

1.2. Légende

Conventions

Les styles utilisés dans ce manuel :

Style	Commentaire
	Notice/indication importante.
	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.



Style	Commentaire
<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 :

- 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,
- -
- 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,
- MIB : base d'information pour la gestion du réseau (Management Information Base),
- 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).

Chapitre 2 : Dr.Web Enterprise Security Suite

2.1. A propos du produit

Dr.Web Enterprise Security Suite est conçu pour la mise en oeuvre d'une protection antivirus unique et 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.

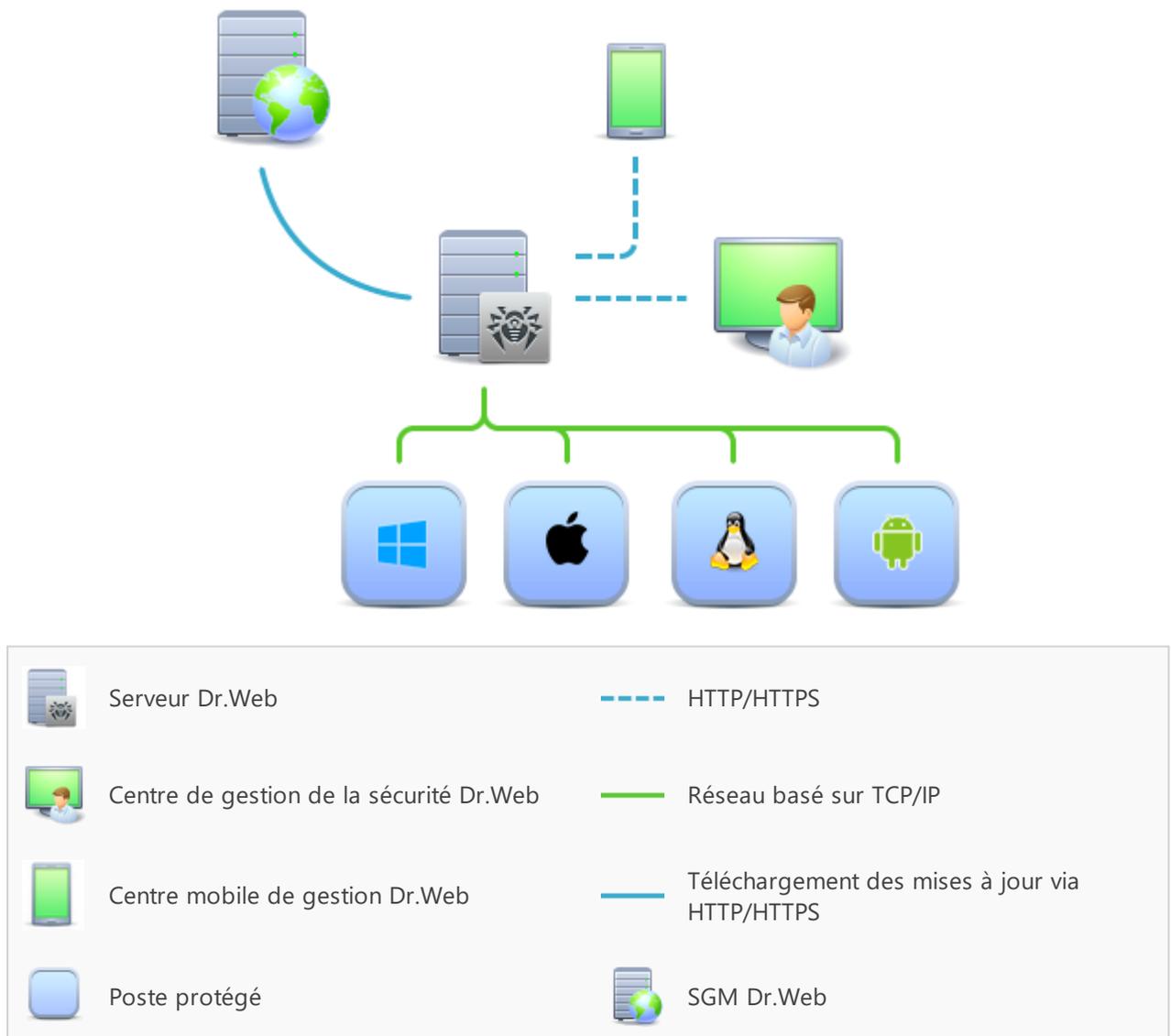


Figure 1-1. Structure logique du réseau antivirus

Le réseau antivirus Dr.Web Enterprise Security Suite a l'architecture *client-serveur*. Ses composants sont installés sur les postes. Dans ce cas, le terme poste signifie un appareils protégé dans le réseau antivirus sur lequel l'Agent Dr.Web et le package antivirus sont installés.



Cet appareil agit en tant que client et interagit avec le Serveur Dr.Web. Ce sont les ordinateurs, les appareils mobiles et virtuels d'utilisateurs et d'administrateurs, les ordinateurs exécutant les fonctions des serveurs LAN qui peuvent jouer le rôle d'un poste.

Les composants du réseau antivirus 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 (ci-après dénommé le Serveur Dr.Web) 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 **Manuel d'installation**, le p. [Pré-requis système](#).

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

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

Le Serveur Dr.Web 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 Dr.Web 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 Dr.Web et contient les statistiques des événements du réseau antivirus, les paramètres du Serveur Dr.Web, 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 (ci-après dénommé le Centre de gestion de la sécurité Dr.Web) s'installe automatiquement avec le Serveur Dr.Web et fournit l'interface Web permettant la gestion à distance du Serveur Dr.Web et du réseau antivirus par le biais de la modification des configurations du Serveur Dr.Web et des postes protégés conservées sur le Serveur Dr.Web et sur les postes protégés.

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

- Windows Internet Explorer,
- Microsoft Edge,



- Mozilla Firefox,
- Google Chrome,
- Navigateur Yandex.

La liste des options d'utilisation possibles se trouve dans le **Manuel d'installation**, p. [Pré-requis système](#).

Le Serveur web est automatiquement installé avec le Serveur Dr.Web 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 mobile de gestion (Dr.Web Mobile Control Center) est fourni en tant que composant à part tournant sous iOS et Android. La configuration requise pour l'application est décrite dans la **Manuel d'installation**, le p. [Pré-requis système](#).

Le Centre de gestion mobile se connecte au Serveur Dr.Web par un protocole crypté et utilise les identifiants de l'administrateur

Vous pouvez télécharger Dr.Web Mobile Control Center 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 Dr.Web) 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 :

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

Les ordinateurs personnels et les serveurs LAN peuvent être considérés comme postes protégés. La protection antivirus du système de messagerie Microsoft Outlook est supportée.

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

En cas d'indisponibilité du Serveur Dr.Web 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 Dr.Web et les postes protégés dans le cas où la connexion directe 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. Le Chargeur du référentiel Dr.Web peut être utilisé pour télécharger les mises à jour de produits Dr.Web Enterprise Security Suite et pour placer les mises à jour sur le Serveur Dr.Web qui n'est pas connecté à Internet.

Serveur de scan Dr.Web

Le serveur de scan Dr.Web est fourni sous forme d'un composant à part destiné à fonctionner dans des environnements virtuels. Le serveur de scan est installé sur une machine virtuelle à part et traite les demandes de scan antivirus reçues des autres machines virtuelles.



2.2. Pré-requis système

Pour l'installation et le fonctionnement de Dr.Web Enterprise Security Suite il faut que :

- Les ordinateurs du réseau antivirus aient un accès au Serveur Dr.Web ou au Serveur proxy Dr.Web.
- Pour assurer l'interaction entre les composants antivirus, les ports suivants doivent être ouverts sur les ordinateurs utilisés :

Numéros de ports	Protocoles	Connexions	Usage
2193	TCP	<ul style="list-style-type: none">• entrantes, sortantes pour le Serveur Dr.Web et le Serveur proxy Dr.Web• sortantes pour l'Agent Dr.Web	Pour l'interaction des composants antivirus avec le Serveur Dr.Web et pour les liaisons entre les serveurs
	UDP	entrantes, sortantes	Le Serveur proxy est également utilisé pour établir une connexion avec les clients Pour le fonctionnement du Scanner du Réseau
139, 445	TCP	<ul style="list-style-type: none">• sortantes pour le Serveur Dr.Web• entrantes pour l'Agent Dr.Web	Pour une installation distante de l'Agent Dr.Web
	UDP	entrantes, sortantes	
9080	HTTP	<ul style="list-style-type: none">• entrantes pour le Serveur Dr.Web• sortantes pour l'ordinateur sur lequel vous ouvrez le Centre de gestion	Pour le fonctionnement du Centre de gestion de la sécurité Dr.Web
9081	HTTPS		
10101	TCP		Pour le fonctionnement de l'utilitaire de diagnostic distant du Serveur Dr.Web
80	HTTP	sortantes	Pour obtenir des mises à jour du SGM
443	HTTPS		
18008	UDP	<ul style="list-style-type: none">• entrantes, sortantes pour le Serveur de scan• entrantes, sortantes pour l'Agent virtuel Dr.Web	Pour la détection de tout Serveur de scan disponible par les Agents virtuels Dr.Web avec l'utilisation du mécanisme Discovery
7090	TCP	<ul style="list-style-type: none">• entrantes pour le Serveur de scan• sortantes pour l'Agent virtuel Dr.Web	Pour la communication des Agents virtuels Dr.Web avec un Serveur de scan particulier



Serveur Dr.Web

Paramètre	Configuration requise
Processeur	CPU avec la prise en charge des instructions SSE2 et la fréquence d'horloge de 1,3 Ghz ou supérieure.
Mémoire vive	<ul style="list-style-type: none">• pré-requis minimum : 1 Go ;• pré-requis recommandés : 2 Go ou plus.
Espace disque	<ul style="list-style-type: none">• 50 Go au minimum pour le logiciel du Serveur Dr.Web et de l'espace supplémentaire pour le stockage des fichiers temporaires, des packages d'installation personnels des Agents (environ 17 Mo chacun) dans le sous-répertoire <code>var\installers-cache</code> du répertoire d'installation du Serveur Dr.Web ;• jusqu' à 5 Go pour la base de données ;• quel que soit l'emplacement d'installation du Serveur Dr.Web, sur le disque système sous Windows ou dans <code>/var/tmp</code> sous les OS de la famille UNIX (ou un autre dossier pour les fichiers temporaire s'il est spécifié) :<ul style="list-style-type: none">▫ l'installation du Serveur Dr.Web requiert 4,3 Go au minimum pour le lancement de l'installateur et l'extraction de fichiers temporaires ;▫ le fonctionnement du Serveur Dr.Web requiert de l'espace libre sur le disque système pour le stockage de fichiers de travail et de fichiers temporaires indépendamment du volume de la base de données et de la configuration du référentiel
Prise en charge d'environnements virtuels et cloud	<p>Le fonctionnement est possible sous les systèmes d'exploitation répondant aux pré-requis listés ci-dessus, dans les environnements virtuels et cloud, y compris :</p> <ul style="list-style-type: none">• VMware,• Hyper-V,• Xen,• KVM,• ECP Veil,• Rosa Virtualization RV2.1
Autre	<p>Pour l'utilisation de la BD Oracle, la bibliothèque <code>Linux kernel AIO access library (libaio)</code> est requise.</p> <p>Les utilitaires de gestion disponibles pour le téléchargement via le Centre de gestion, section Administration → Utilitaires) doivent être lancés sur l'ordinateur possédant la configuration requise par le Serveur Dr.Web</p>



Le Serveur Dr.Web ne peut pas être installé sur les disques logiques avec les systèmes de fichiers qui ne prennent pas en charge les liens symboliques, en particulier, avec les systèmes de fichiers de la famille FAT.

Le Serveur Dr.Web ne peut pas être installé sur le même poste que le Serveur proxy Dr.Web.

Pour installer sur Alt Linux, il faut désactiver SELinux.

Pour installer le Serveur Dr.Web et le Serveur proxy Dr.Web sous les OS de la famille UNIX, il faut que le système d'initialisation SysVinit soit pris en charge par le système d'exploitation. Si ce n'est pas le cas, il faut installer le package correspondant.

Liste des systèmes d'exploitation pris en charge :

Windows	UNIX
<p><i>Pour les systèmes 32 bits :</i></p> <ul style="list-style-type: none">• Windows 7,• Windows 8,• Windows 8.1,• Windows 10. <p><i>Pour les systèmes 64 bits :</i></p> <ul style="list-style-type: none">• Windows Server 2008 R2,• Windows 7,• Windows Server 2012,• Windows Server 2012 R2,• Windows 8,• Windows 8.1,• Windows 10,• Windows 11,• Windows Server 2016,• Windows Server 2019,• Windows Server 2022	<ul style="list-style-type: none">• Linux, en cas de présence de la bibliothèque glibc 2.13 ou une version supérieure,• FreeBSD 11.3 ou une version supérieure. <p>Ainsi que les versions spéciales des distributions de Linux :</p> <ul style="list-style-type: none">▪ Alt Linux 8,▪ Alt Linux 9,▪ Astra Linux Special Edition 1.5 (avec le correctif cumulatif 20201201SE15),▪ Astra Linux 1.6 (avec le correctif cumulatif 20200722SE16),▪ Astra Linux 1.7,▪ Astra Linux Common Edition 2.12 Orel,▪ Alt 8 SP,▪ Goslinux IC6,▪ RED OS 7.3 MUROM. <p>Sous Alt 8 SP et Goslinux IC6 le contrôle d'accès obligatoire n'est pas supporté.</p>

Serveur proxy Dr.Web

Paramètre	Configuration requise
Processeur	CPU avec la prise en charge des instructions SSE2 et la fréquence d'horloge de 1,3 Ghz ou supérieure.



Paramètre	Configuration requise
Mémoire vive	1 Go au minimum
Espace disque	1 Go au minimum
Système d'exploitation	La liste des systèmes d'exploitation correspond à celle du Serveur Dr.Web



Le Serveur proxy Dr.Web ne peut pas être installé sur le même poste que le Serveur Dr.Web.

Centre de gestion de la sécurité Dr.Web

Paramètre	Configuration requise
Navigateur	Un des navigateurs suivants : <ul style="list-style-type: none">• Internet Explorer 11,• Microsoft Edge 0.10 ou une version supérieure,• Mozilla Firefox 44 ou une version supérieure,• Google Chrome 49 ou une version supérieure,• Opera en dernière version,• Safari en dernière version,• Yandex Browser en dernière version
Résolution de l'écran	Résolution de l'écran recommandée — 1280x1024
Autre	En cas d'utilisation du navigateur web Windows Internet Explorer, il faut prendre en compte les particularités suivantes : <ul style="list-style-type: none">• le fonctionnement complet du Centre de gestion sous le navigateur web Windows Internet Explorer avec le mode Enhanced Security Configuration for Windows Internet Explorer activé n'est pas garanti ;• si vous installez le Serveur Dr.Web sur un ordinateur comportant le caractère « _ » (souligné) dans son nom, la configuration du Serveur via le Centre de gestion sera impossible. Dans ce cas, utilisez un autre navigateur web ;• pour un fonctionnement correct du Centre de gestion, l'adresse IP et/ou le nom DNS de l'ordinateur sur lequel est installé le Serveur Dr.Web doivent être ajoutés à la liste des sites de confiance du navigateur web dans lequel vous ouvrez le Centre de gestion ;• pour une ouverture correcte du Centre de gestion via le menu Démarrer sous Windows 8 et Windows Server 2012 avec une interface en mosaïque, configurez le navigateur web de manière suivante : Options Internet → Programmes → Ouvrir Internet Explorer cochez la case Toujours dans Internet Explorer sur le Bureau ;



- pour une interaction correcte avec le Centre de gestion via le navigateur web Windows Internet Explorer par le protocole sécurisé https, il faut installer toutes les dernières mises à jour du navigateur web ;
- la gestion du Centre de gestion via le navigateur web Windows Internet Explorer n'est pas prise en charge en mode de compatibilité



Si votre organisation utilise un serveur proxy inverse (reverse proxy) pour accéder au Centre de gestion de la sécurité Dr.Web, les paramètres supplémentaires sont requis. Pour voir les exemples des paramètres, consultez les liens suivants :

Pour Nginx :

<https://nginx.org/docs/http/websocket.html>

Pour Apache :

https://httpd.apache.org/docs/2.4/mod/mod_proxy_wstunnel.html

<https://www.serverlab.ca/tutorials/linux/web-servers-linux/how-to-reverse-proxy-websockets-with-apache-2-4/>

Centre mobile de gestion Dr.Web

Système d'exploitation	Configuration requise	
	Version de système d'exploitation	Appareil
iOS	iOS 9 ou une version supérieure	<ul style="list-style-type: none">• Apple iPhone,• Apple iPad
Android	Android 5.0-12	–

NAP Validator

Paramètre	Configuration requise	
	Pour le Serveur Dr.Web	Pour l'Agent Dr.Web
Système d'exploitation	Windows Server 2008	<ul style="list-style-type: none">• Windows XP SP3,• Windows Vista avec SP2
Autre	La configuration requise pour NAP Validator correspond à celle de l'Agent Dr.Web. Les pré-requis peuvent varier en fonction du système d'exploitation sous lequel la solution antivirus est installée	



Serveur de scan Dr.Web

Paramètre	Configuration requise
Processeur	Processeurs avec architecture et système de commandes Intel/AMD : 32 bits (IA-32, x86) ; 64 bits (x86_64, x64, AMD64).
Mémoire vive	500 Mo au minimum (il est recommandé d'avoir 1 Go et plus)
Espace disque	1 Go d'espace disque disponible au minimum
Hyperviseur	<ul style="list-style-type: none">• VMware,• Hyper-V,• Xen,• KVM
Système d'exploitation	Linux, FreeBSD. La liste des systèmes d'exploitation pris en charge correspond à celle du package antivirus pour l'OS UNIX
Connexions réseau	Les connexions réseau suivantes sont requises : <ul style="list-style-type: none">• connexion au Serveur Dr.Web pour la mise à jour des bases virales et des bases des filtres intégrés ;• connexion pour le traitement des requêtes des agents virtuels

Agent Dr.Web et package antivirus

Les pré-requis varient en fonction du système d'exploitation sur lequel la solution antivirus est installée.



Aucun autre logiciel antivirus (y compris d'autres versions de Dr.Web, des pare-feux ou des logiciels de filtrage du contenu Web) ne doit être utilisé sur les postes dans le réseau antivirus géré par Dr.Web Enterprise Security Suite.

Windows

Paramètre	Pré-requis
Processeur	Avec la prise en charge du système de commandes i686



Paramètre	Pré-requis
Système d'exploitation	<p>Pour les systèmes d'exploitation 32 bits :</p> <ul style="list-style-type: none">• Windows XP avec SP2 ou une version supérieure ;• Windows Vista avec SP2 ou une version supérieure ;• Windows 7 avec SP1 ou une version supérieure ;• Windows 8 ;• Windows 8.1 ;• Windows 10 22H2 ou une version antérieure ;• Windows Server 2003 avec SP1 ;• Windows Server 2008 avec SP2 ou une version supérieure. <p>Pour les systèmes d'exploitation 64 bits :</p> <ul style="list-style-type: none">• Windows Vista avec SP2 ou une version supérieure ;• Windows 7 avec SP1 ou une version supérieure ;• Windows 8 ;• Windows 8.1 ;• Windows 10 22H2 ou une version antérieure ;• Windows 11 22H2 ou une version antérieure ;• Windows Server 2008 avec SP2 ou une version supérieure ;• Windows Server 2008 R2 avec SP1 ou une version supérieure ;• Windows Server 2012 ;• Windows Server 2012 R2 ;• Windows Server 2016 ;• Windows Server 2019 ;• Windows Server 2022
Mémoire vive disponible	512 Mo ou plus
Résolution de l'écran	Au moins 1024x768 recommandé
Prise en charge d'environnements virtuels et cloud	<p>Le programme fonctionne dans les environnements suivants :</p> <ul style="list-style-type: none">• VMware ;• Hyper-V ;• Xen ;• KVM
Autre	<p>Une connexion au serveur de la protection centralisée ou Internet dans le mode mobile est requise pour mettre à jour les bases virales Dr.Web et les composants de Dr.Web.</p> <p>Le plug-in Dr.Web pour Microsoft Outlook nécessite l'installation du client Microsoft Outlook intégré dans Microsoft Office :</p> <ul style="list-style-type: none">• Outlook 2000 ;



Paramètre	Pré-requis
	<ul style="list-style-type: none">• Outlook 2002 ;• Outlook 2003 ;• Outlook 2007 ;• Outlook 2010 avec SP2 ;• Outlook 2013 ;• Outlook 2016 ;• Outlook 2019 ;• Outlook 2021

UNIX

Composant	Pré-requis
Plateforme	Les processeurs avec les architectures et les systèmes de commandes suivants sont pris en charge : <ul style="list-style-type: none">• Intel/AMD : 32 bits (<i>IA-32, x86</i>) ; 64 bits (<i>x86-64, x64, amd64</i>) ;• ARM64 ;• E2K (<i>Elbrus</i>) ;• IBM POWER (<i>ppc64el</i>)
Mémoire vive	500 Mo au minimum (il est recommandé d'avoir 1 Go et plus)
Espace disque	Au moins 2 Go d'espace disque libre sur le volume qui contient les répertoires du produit installé
Système d'exploitation	GNU/Linux (basé sur le noyau 2.6.37 ou une version supérieure, utilisant la bibliothèque <code>glibc</code> en version 2.13 ou une version supérieure, le système d'initialisation <code>systemd</code> en version 209 ou une version supérieure), FreeBSD. Vous trouverez ci-dessous la liste des versions des systèmes d'exploitation prises en charge. Le système d'exploitation doit prendre en charge le mécanisme d'authentification PAM
Autre	Les connexions réseau suivantes sont requises : <ul style="list-style-type: none">• connexion Internet pour la mise à jour des bases virales et des composants du produit antivirus ;• en mode de protection centralisée, il suffit d'avoir une connexion au serveur via un réseau local ; une connexion Internet n'est pas requise

Plateforme	Versions GNU/Linux prises en charge
x86_64	<ul style="list-style-type: none">• Astra Linux Special Edition 1.5 (avec le correctif cumulatif 20201201SE15), 1.6 (avec le correctif cumulatif 20200722SE16),



Plateforme	Versions GNU/Linux prises en charge
	<ul style="list-style-type: none">1.7 ;• Astra Linux Common Edition (Orel) 2.12 ;• Debian 9, 10 ;• Fedora 31, 32 ;• CentOS 7, 8 ;• Ubuntu 18.04, 20.04, 22.04 ;• Alt Poste de travail 9, 10 ;• Alt Serveur 9, 10 ;• Alt 8 SP ;• RED OS 7.2 MUROM, RED OS 7.3 MUROM ;• Goslinux IC6 ;• SUSE Linux Enterprise Server 12 SP3 ;• Red Hat Enterprise Linux 7, 8
x86	<ul style="list-style-type: none">• CentOS 7 ;• Debian 10 ;• Alt Poste de travail 9, 10 ;• Alt 8 SP
ARM64	<ul style="list-style-type: none">• Ubuntu 18.04 ;• CentOS 7, 8 ;• Alt Poste de travail 9, 10 ;• Alt Serveur 9, 10 ;• Alt 8 SP ;• Astra Linux Special Edition (Novorossiysk) 4.7
E2K	<ul style="list-style-type: none">• Astra Linux Special Edition (Leningrad) 8.1 (avec le correctif cumulatif 20200429SE81) ;• Alt 8 SP ;• Elbrus-D MCST 1.4 ;• GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	<ul style="list-style-type: none">• CentOS 8 ;• Ubuntu 20.04 ;



Sous Alt 8 SP, Astra Linux Special Edition (Novorossiysk) 4.11 et Goslinux IC6, le contrôle d'accès obligatoire n'est pas supporté.

La compatibilité complète d'autres distributions Linux correspondant aux pré-requis décrits n'est pas garantie. En cas de problème de compatibilité avec votre distribution, contactez le support technique : <https://support.drweb.com>.



Plateforme	Versions FreeBSD prises en charge
x86	11, 12, 13
x86_64	11, 12, 13



Sous FreeBSD, l'installation de l'application se fait uniquement depuis le package universel.

macOS

Paramètre	Configuration requise
Appareil	Mac tournant sous le système d'exploitation macOS
Espace disque	2 Go
Système d'exploitation	<ul style="list-style-type: none">• OS X 10.11 El Capitan ;• macOS 10.12 Sierra ;• macOS 10.13 High Sierra ;• macOS 10.14 Mojave ;• macOS 10.15 Catalina ;• macOS 11 Big Sur ;• macOS 12 Monterey ;• macOS 13 Ventura.

OS Android

Paramètre	Pré-requis
Système d'exploitation	Android en version 4.4 - 14.0 Android TV (sur les téléviseurs, les lecteurs média et les consoles de jeux)
Processeur	x86/x86-64/ARMv7/ARMv8/ARMv9
Mémoire vive disponible	512 Mo au minimum
Espace disque disponible	45 Mo au minimum (pour le stockage de données)
Résolution de l'écran	800x480 au minimum
Autre	Connexion Internet (pour la mise à jour des bases virales). Le mode de protection centralisée n'est pas disponible sur les



Paramètre	Pré-requis
	appareils tournant sous Android TV

Dr.Web pour Exchange Server

Paramètre	Pré-requis
Mémoire vive disponible	512 Mo ou plus
Espace disque disponible	1 Go et plus
Système d'exploitation	<ul style="list-style-type: none">• Windows Server 2008 x64 avec SP2 installé ;• Windows Server 2008 R2 ;• Windows Server 2012 ;• Windows Server 2012 R2 ;• Windows Server 2016 ;• Windows Server 2019 ;• Windows Server 2022
Version de Microsoft Exchange Server	<ul style="list-style-type: none">• Microsoft Exchange Server 2007 x64 avec SP1 installé ;• Microsoft Exchange Server 2010 x64 avec SP1 installé ;• Microsoft Exchange Server 2013 avec SP1 installé (l'installation supplémentaire de Cumulative Update 5 ou le lancement du script Exchange2013-KB2938053-Fixit est requis) ;• Microsoft Exchange Server 2016 avec Cumulative Update 3 installé (ou une version supérieure) ;• Microsoft Exchange Server 2019

Dr.Web pour Lotus Domino

Paramètre	Pré-requis
Processeur	Compatible avec le système de commandes i686
Mémoire vive	512 Mo ou plus
Espace disque	750 Mo ou plus. Les fichiers temporaires créés pendant l'installation nécessitent encore de l'espace libre
Résolution de l'écran	Il est recommandé d'avoir au moins 1280×1024 avec la prise en charge du mode 256 couleurs au minimum



Paramètre	Pré-requis
Système de fichiers	NTFS ou FAT32
Système d'exploitation	Pour les systèmes 32 bits : <ul style="list-style-type: none">• Windows Server 2008,• Windows Server 2008 R2. Pour les systèmes 64 bits : <ul style="list-style-type: none">• Windows Server 2008,• Windows Server 2008 R2,• Windows Server 2012,• Windows Server 2012 R2,• Windows Server 2016,• Windows Server 2019,• Windows Server 2022
Autres systèmes	Lotus : <ul style="list-style-type: none">• IBM Lotus Domino pour Windows en version 8.5 - 9.0.1,• IBM Lotus Notes pour Windows en version 7.0.2 - 9.0.1,• IBM Domino pour Windows 10.1,• IBM Notes pour Windows 10.0,• HCL Domino pour Windows 11.0,• HCL Notes pour Windows 11.0. Navigateurs pour la gestion de l'interface web : <ul style="list-style-type: none">• Google Chrome 8 ou une version supérieure ;• Mozilla Firefox 3 ou une version supérieure,• Opera 9 ou une version supérieure

2.3. Kit de distribution

La distribution Dr.Web Enterprise Security Suite est fournie en fonction du système d'exploitation du Serveur Dr.Web sélectionné :

1. 'Pour les OS de la famille UNIX :

- `drweb-esuite-server-<version_du_package>-<assemblage>-<version_de_l'OS>.tar.gz.run`

Distribution du Serveur Dr.Web.

- `drweb-reloader-<OS>-<nombre de bits>`

Version de console du Chargeur du référentiel Dr.Web.



2. Sous Windows :

- `drweb-esuite-server-<version_du_package>-<assemblage>-<version_de_l'OS>.exe`
Distribution du Serveur Dr.Web.
- `drweb-<version_du_package>-<assemblage>-esuite-agent-full-windows.exe`
Installateur complet de l'Agent Dr.Web.
- `drweb-reloader-windows-<nombre_de_bits>.exe`
Version de console du Chargeur du référentiel Dr.Web.
- `drweb-reloader-gui-windows-<nombre_de_bits>.exe`
Version graphique du Chargeur du référentiel Dr.Web.

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

- logiciel du Serveur Dr.Web pour le système d'exploitation correspondant ;
- données de sécurité du Serveur Dr.Web ;
- logiciel du Centre de gestion de la sécurité Dr.Web ;
- logiciel de l'Agent Dr.Web et package antivirus pour les postes sous Windows ;
- module de mise à jour de l'Agent Dr.Web pour Windows ;
- Antispam Dr.Web pour Windows ;
- bases virales, bases de filtres intégrés des composants antivirus et de l'Antispam Dr.Web pour Windows ;
- documentation ;
- actualités de Doctor Web.

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

Après l'installation du Serveur Dr.Web, vous pourrez télécharger dans le référentiel les Produits d'entreprise Dr.Web suivants se trouvant sur les serveurs du SGM :

- Produits pour l'installation sur les postes protégés tournant sous UNIX (y compris les serveurs du réseau local), Android, macOS ;
- Serveur de scan Dr.Web ;
- Dr.Web pour IBM Lotus Domino ;
- Dr.Web pour Microsoft Exchange Server ;
- Serveur proxy Dr.Web ;
- Installateur complet de l'Agent Dr.Web pour Windows ;
- Agent Dr.Web pour Active Directory ;
- Utilitaire de modification du schéma Active Directory ;
- Utilitaire de modification des attributs des objets Active Directory ;



- NAP Validator.



Pour en savoir plus sur la gestion du référentiel du Serveur Dr.Web, consultez le **Manuel Administrateur**, la rubrique [Gestion du référentiel du Serveur Dr.Web](#).



Chapitre 3 : 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, les machines virtuelles 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 de protection centralisée peut être installé sur n'importe quel ordinateur et pas uniquement sur le poste utilisé comme serveur LAN. Pour en savoir plus sur les pré-requis principaux, consultez le **Manuel d'installation**, le p. [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 Dr.Web.

Pour installer le Serveur Dr.Web et l'Agent Dr.Web une procédure d'accès unitaire aux postes 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.

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.

Vous pouvez consulter la description détaillée de l'ordre de gestion des groupes administratifs et des règles d'accès dans le **Manuel Administrateur**, [Chapitre 6 : Administrateurs du réseau antivirus](#).

2. Déterminez quels produits pour quels systèmes d'exploitation sont 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 le site de Doctor Web <https://download.drweb.com/>.



Les Agents Dr.Web pour les postes 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 Dr.Web 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 Dr.Web. Par défaut, le Serveur Dr.Web démarre de manière automatique après l'installation et après chaque redémarrage du système.
4. Si nécessaire, installez et configurez le Serveur proxy. Vous pouvez consulter la description dans le **Manuel d'installation**, le p. [Installation du Serveur proxy Dr.Web](#).
5. Si le réseau antivirus est composé de machines virtuelles, il est recommandé d'utiliser le Serveur de scan. Vous trouverez la description d'installation et de configuration dans le **Manuel d'installation**, p. [Installation du Serveur de scan Dr.Web](#).
6. Pour configurer le Serveur Dr.Web et le logiciel antivirus sur les postes, il faut se connecter au Serveur Dr.Web 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 Dr.Web. Une connexion réseau doit être établie avec l'ordinateur sur lequel le Serveur Dr.Web est installé.

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

`http://<Adresse_du_Serveur_Dr.Web>:9080`

ou

`https://<Adresse_du_Serveur_Dr.Web>:9081`

où comme valeur `<Adresse_du_Serveur_Dr.Web>` spécifiez l'adresse IP, NetBIOS 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 Dr.Web.
 - pour les OS de la famille UNIX — mot de passe qui a été automatiquement créé au cours de l'installation du Serveur Dr.Web (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 Dr.Web 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](#)).

Si vous avez installé le Serveur de scan, indiquez son adresse dans les paramètres du poste (voir la description détaillée dans le **Manuel Administrateur**, p. [Connexion de postes au Serveur de scan](#)).



7. Effectuez la configuration initiale du Serveur Dr.Web (vous pouvez consulter le description détaillée des paramètres dans le **Manuel Administrateur**, dans la [Chapitre 10 : 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 Dr.Web.
 - b. Dans la rubrique [Configuration générale du référentiel](#), spécifiez les composant du réseau antivirus à mettre à jour depuis le SGM Dr.Web. Si le réseau antivirus inclut des postes protégés sous Android, Linux, macOS, il faut télécharger les **produits d'entreprise Dr.Web**.

Dans la rubrique [Statut du référentiel](#) effectuez la mise à jour des produits du référentiel du Serveur Dr.Web. La mise à jour peut prendre un long temps. Attendez la fin de la mise à jour avant de continuer la configuration.



Lors de l'installation du Serveur Dr.Web en version 13, les mises à jour des produits de référentiel **Bases Dr.Web pour Android**, **Agent Dr.Web pour UNIX** et **Serveur proxy Dr.Web** sont téléchargées depuis le SGM uniquement en cas d'appel de ces produits depuis les postes. Pour en savoir plus, consultez le **Manuel Administrateur**, le p. [Configuration détaillée du référentiel](#).

Si votre Serveur Dr.Web n'est pas connecté à Internet, les mises à jour sont téléchargées manuellement depuis un autre Serveur Dr.Web ou via le Chargeur du référentiel et que vous voulez installer ou mettre à jour les produits pour lesquels l'option **Mettre à jour à la demande uniquement** est activé dans le paramètres du référentiel, il faut d'abord télécharger ces produits manuellement dans le référentiel.

- c. Vous trouverez les informations sur la version du Serveur Dr.Web sur la page **Administration** → **Serveur Dr.Web**. Si la nouvelle version est disponible, mettez à jour le Serveur Dr.Web. 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, spécifiez la [Configuration des 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 Dr.Web. L'authentification externe des administrateurs est également possible. Pour en savoir plus, consultez le **Manuel Administrateur**, la [Chapitre 6 : 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 Dr.Web (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 Dr.Web et de ceux de la copie de sauvegarde.



8. Spécifiez les paramètres et la configuration du logiciel antivirus pour les postes (vous pouvez consulter la description détaillée de la configuration de groupes et de postes dans le **Manuel Administrateur**, la [Chapitre 7](#) et la [Chapitre 8](#)) :
 - a. Si nécessaire, créez les groupes utilisateur de postes.
 - b. Spécifiez les paramètres du groupe **Everyone** et des groupes utilisateur créés. Notamment configurez la rubrique des composants à installer.

9. Installez le logiciel de l'Agent Dr.Web sur un poste.

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

- Si 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 Dr.Web.
- 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 poste ou sur plusieurs postes en même temps tournant sous Windows ou Linux. 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 Dr.Web.
- Si, lors de l'installation, il faut diminuer la charge sur le canal de communication entre le Serveur Dr.Web et les postes, vous pouvez utiliser l'installateur complet qui effectue l'installation de l'Agent Dr.Web et des composants de protection en même temps.
- L'installation sur les postes sous OS Android et macOS peut s'effectuer de manière locale conformément aux règles générales. Le produit autonome installé peut se connecter au Serveur Dr.Web conformément à la configuration correspondante.



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 Dr.Web se connectent automatiquement au Serveur Dr.Web. L'approbation des postes antivirus sur le Serveur Dr.Web 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 Dr.Web, les postes sont enregistrés automatiquement à la première connexion au Serveur Dr.Web 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 Dr.Web. Dans ce cas, les nouveaux postes ne se connectent pas automatiquement, mais ils sont déplacés par le Serveur Dr.Web dans le groupe de novices.
11. Après la connexion au Serveur Dr.Web 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 antivirus est également possible après l'installation (vous pouvez consulter la description détaillée dans le **Manuel Administrateur**, dans la [Chapitre 8](#)).



Annexe A. Octroi de 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/v4/>, 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 les 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 les fichiers clés de démo, vous devez remplir un formulaire se trouvant sur la page <https://download.drweb.com/demoreq/biz/>. Votre demande sera traitée à titre individuel. En cas de réponse positive, une archive contenant les fichiers clés de licence vous sera envoyée à l'adresse e-mail indiquée.



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 [Octroi de 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 :

1. Consultez les dernières versions des descriptions et des manuels à l'adresse <https://download.drweb.com/doc/>.
2. Lisez la rubrique de questions fréquentes à l'adresse https://support.drweb.com/show_faq/.
3. 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 :

1. Remplissez le formulaire de question dans la section correspondante de la rubrique <https://support.drweb.com/>.
2. Appelez le numéro de l'assistance technique française 0 825 300 230 ou le numéro de l'assistance internationale +7 (495) 789 45 86. Les utilisateurs en Russie peuvent nous contacter en appelant le numéro vert 8 800 333 7932.

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/>.

