



Dr.WEB

Enterprise Security Suite

Manuel d'Installation



© **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
Manuel d'Installation
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	6
1.1. Destination du document	6
1.2. Légende et abréviations	7
Chapitre 2 : Dr.Web Enterprise Security Suite	9
2.1. A propos du produit	9
2.2. Pré-requis système	19
2.3. Kit de distribution	31
Chapitre 3 : Octroi de licence	33
Chapitre 4 : Mise en route	35
4.1. Création d'un réseau antivirus	35
4.2. Configuration des connexions réseau	39
4.2.1. Connexions directes	40
4.2.2. Service de détection du Serveur Dr.Web	41
4.2.3. Utiliser le protocole SRV	42
4.3. Assurance d'une connexion sécurisée	43
4.3.1. Chiffrement et compression du trafic	43
4.3.2. Instruments assurant une connexion sécurisée	49
4.3.3. Connexion des clients au Serveur Dr.Web	51
4.4. Intégration de Dr.Web Enterprise Security Suite avec Active Directory	53
Chapitre 5 : Installation des composants Dr.Web Enterprise Security Suite	56
5.1. Installation du Serveur Dr.Web	56
5.1.1. Installation du Serveur Dr.Web sous Windows	57
5.1.2. Installation du Serveur Dr.Web pour les OS de la famille UNIX	64
5.2. Installation de l'Agent Dr.Web	65
5.2.1. Fichiers d'installation	67
5.2.2. Installation de l'Agent Dr.Web en mode local	70
5.2.3. Installation de l'Agent Dr.Web à distance	82
5.3. Installation du Serveur de scan Dr.Web	100
5.4. Installation de NAP Validator	101
5.5. Installation du Serveur proxy Dr.Web	102
5.5.1. Création d'un compte du Serveur proxy Dr.Web	103
5.5.2. Installation du Serveur proxy Dr.Web lors de l'installation de l'Agent Dr.Web pour Windows	105



5.5.3. Installation du Serveur proxy Dr.Web avec l'installateur	106
5.5.4. Connexion du Serveur proxy Dr.Web au Serveur Dr.Web	110
5.6. Codes d'erreur retournés lors de l'installation	113
Chapitre 6 : Suppression des composants Dr.Web Enterprise Security Suite	115
6.1. Suppression du Serveur Dr.Web	115
6.1.1. Suppression du Serveur Dr.Web sous Windows	115
6.1.2. Suppression du Serveur Dr.Web sous les OS de la famille UNIX	115
6.2. Suppression de l'Agent Dr.Web	116
6.2.1. Suppression de l'Agent Dr.Web pour Windows	117
6.2.2. Suppression de l'Agent Dr.Web avec le service Active Directory	120
6.3. Suppression du Serveur de scan Dr.Web	121
6.4. Suppression du Serveur proxy Dr.Web	121
6.4.1. Suppression locale du Serveur proxy Dr.Web	122
6.4.2. Suppression à distance du Serveur proxy Dr.Web	123
Chapitre 7 : Mise à jour des composants de Dr.Web Enterprise Security Suite	125
7.1. Mise à jour du Serveur Dr.Web sous Windows	126
7.2. Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX	130
7.3. Mise à jour des Agents Dr.Web	134
7.3.1. Mise à jour des Agents Dr.Web sur les postes tournant sous Windows	134
7.3.2. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Android	137
7.3.3. Mise à niveau des Agents Dr.Web sur les postes tournant sous Linux et macOS	138
7.4. Mise à jour du Serveur proxy Dr.Web	138
7.4.1. Mise à jour du Serveur proxy Dr.Web lors de son fonctionnement	138
7.4.2. Mise à jour du Serveur proxy Dr.Web via l'installateur	139
Référence	142



Chapitre 1 : Introduction

1.1. Destination du document

La documentation de l'administrateur du réseau antivirus Dr.Web Enterprise Security Suite décrit les principes généraux ainsi que les détails concernant la mise en oeuvre de la protection antivirus des ordinateurs d'entreprise avec Dr.Web Enterprise Security Suite.

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

1. Manuel d'installation

Le Manuel d'installation sera utile à la personne responsable de l'achat et de l'installation d'un système de protection antivirus complète.

Le Manuel d'installation explique comment construire un réseau antivirus et installer ses composants.

2. Manuel Administrateur

Le Manuel Administrateur s'adresse à *l'administrateur du réseau antivirus*, la personne qui est responsable dans l'entreprise de la protection antivirus des ordinateurs (postes et serveurs) de ce réseau.

L'administrateur du réseau antivirus doit posséder les privilèges administrateur sur le système ou collaborer avec l'administrateur du réseau local, savoir mettre en place la politique de protection antivirus et connaître en détails les packages antivirus Dr.Web pour tous les systèmes d'exploitation utilisés dans le réseau.

3. Annexes

Les Annexes fournissent des informations techniques, décrivent les paramètres de configuration des composants Antivirus, ainsi que la syntaxe et les valeurs utilisées pour leur gestion.



La documentation contient des renvois entre les documents mentionnés ci-dessus. Si vous téléchargez ces documents sur un ordinateur local, les renvois fonctionnent uniquement si les documents se trouvent dans le même dossier et portent leurs noms initiaux.

De plus, les manuels suivants sont fournis :

1. Instructions de déploiement du réseau antivirus

Les instructions contiennent de brèves informations sur l'installation et la configuration initiale des composants du réseau antivirus. Pour des informations détaillées, consultez la documentation de l'administrateur.



2. Manuels de gestion des postes

Ces manuels contiennent les informations sur la configuration centralisée des composants du logiciel antivirus sur les postes effectuée par l'administrateur du réseau antivirus via le Centre de gestion de la sécurité Dr.Web.

3. Manuels Utilisateur

Les manuels utilisateur contiennent les informations sur la configuration de la solution antivirus Dr.Web effectuée directement sur les postes protégés.

4. Manuel sur Web API

Il contient les informations techniques sur l'intégration de Dr.Web Enterprise Security Suite avec un tiers logiciel via Web API.

5. Manuel de la structure de la base de données du Serveur Dr.Web

Contient la description de la structure interne de la base de données du Serveur Dr.Web et des exemples de son utilisation.



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 et abréviations

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.
<IP-address>	Champs destinés à remplacer les noms fonctionnels par leurs valeurs.
Enregistrer	Noms des boutons de l'écran, des fenêtres, des éléments de menu et d'autres éléments de l'interface du logiciel.
CTRL	Touches du clavier.



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

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.

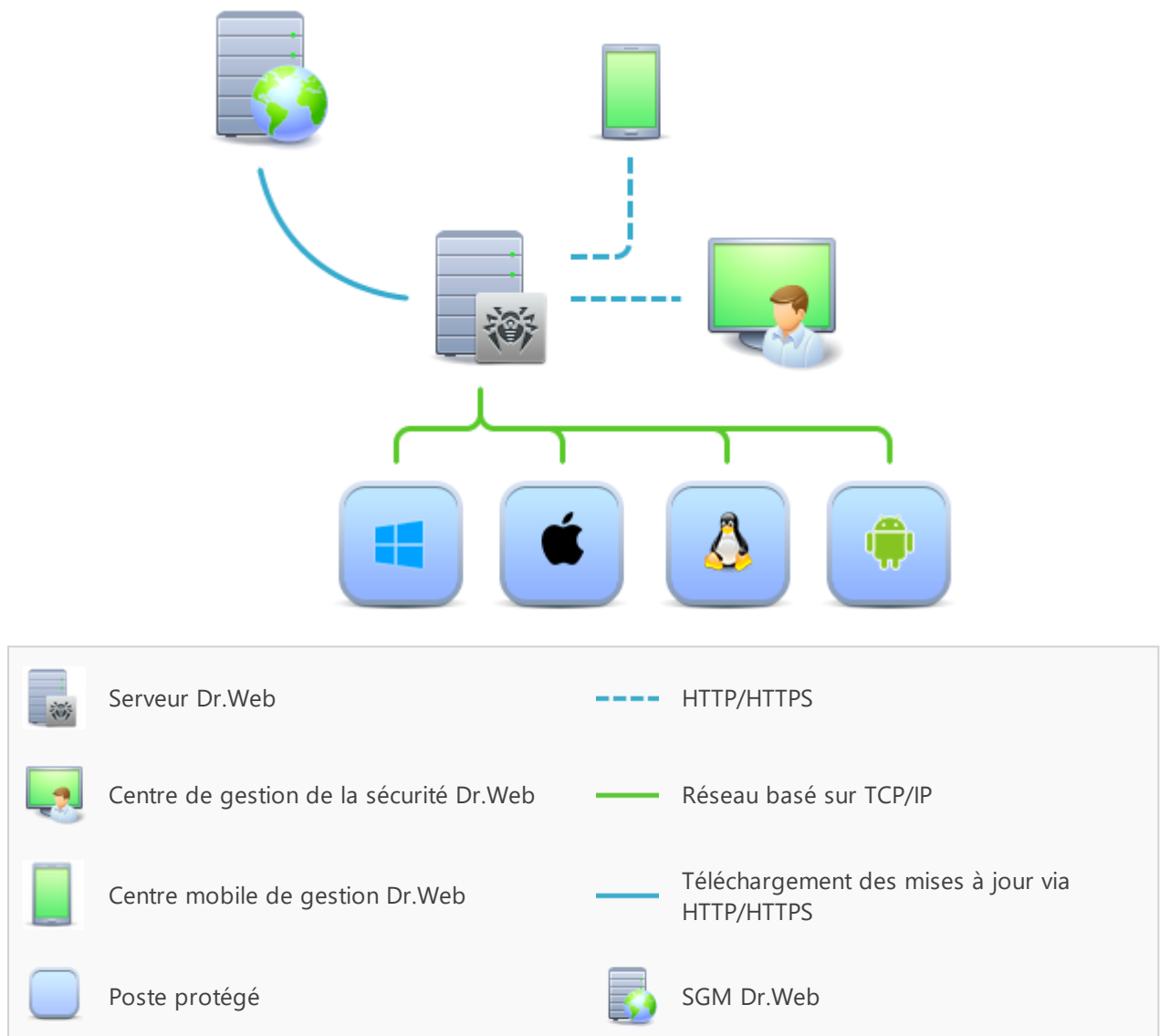


Figure 1-1. Structure logique du réseau antivirus

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.

Il est possible de créer la structure hiérarchique contenant plusieurs Serveurs Dr.Web qui maintiennent les postes protégés du réseau antivirus.

Le Serveur Dr.Web prend en charge la fonction de sauvegarde (backup) des données critiques (les bases de données, fichiers de configuration etc.).

Le Serveur Dr.Web effectue la journalisation des événements du réseau antivirus.

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.

Les types suivants de bases de données peuvent être utilisés :

Base de données embarquée. La base de données SQLite3 embarquée directement dans le Serveur Dr.Web est fournie.

Base de données externe. Les pilotes intégrés pour la connexion des bases de données suivantes sont fournis :

- MySQL, Maria DB,
- Oracle,



- PostgreSQL (PostgreSQL Pro, Jatoba et autres),
- Pilote ODBC pour connecter d'autres bases de données, comme Microsoft SQL Server/Microsoft SQL Server Express.

Vous pouvez utiliser n'importe quelle base de données correspondant à vos besoins tels que : la possibilité de maintenir le réseau antivirus d'une taille correspondante, les particularités de maintenance du logiciel de la base de données, les possibilités d'administration fournies par la base de données et d'autres exigences et normes adoptées dans votre entreprise.

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 conservés 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 Centre de gestion fournit les fonctionnalités suivantes :

- Facilité d'installation de l'Antivirus sur les postes protégés, y compris la possibilité d'installation à distance avec une recherche préliminaire des ordinateurs ; création de distributions aux identifiants et aux paramètres uniques de connexion au Serveur de protection centralisée pour faciliter le processus d'installation de l'Antivirus par l'administrateur et donner la possibilité aux utilisateurs d'installer l'Antivirus eux-même (pour plus d'informations, voir [Installation de l'Agent Dr.Web](#)).
- Facilité de gestion des postes dans le réseau antivirus, assurée par un mécanisme de groupement.
- Possibilité de gestion centralisée de packages antivirus de postes, y compris : suppression de composants particuliers ou de l'Antivirus dans son ensemble sur les postes tournant sous l'OS Windows ; configuration de paramètres de composants de packages antivirus ; spécification de droits d'utilisateurs de configurer et gérer les packages antivirus sur les postes protégés.
- Gestion centralisée du scan antivirus de postes, y compris lancement à distance du scan antivirus selon la planification ou la requête directe de l'administrateur depuis le



Centre de gestion, configuration centralisée de paramètres du scan antivirus qui sont transmis sur les postes pour lancer le scan local avec les paramètres spécifiés.

- Obtention des informations statistiques sur le statut de postes protégés, statistiques virales, statut du logiciel installé, statut des composants lancés et liste de hardware et software du poste protégé.
- Système flexible d'administration du Serveur de protection centralisée et du réseau antivirus grâce à la possibilité de délimiter les droits des administrateurs différents, possibilité de connexion des administrateurs via les systèmes d'authentification externes comme par exemple Active Directory, LDAP, RADIUS, PAM.
- Gestion de licences de protection antivirus sur les postes avec le système ramifié d'assignation de licences aux postes, groupes de postes et de transmission de licences entre plusieurs Serveurs de protection centralisée en cas de configuration réseau multi-serveurs.
- Un large ensemble de paramètres pour configurer le Serveur Dr.Web et ses composants, y compris : configuration de planification de maintenance ; ajout de procédures utilisateur ; configuration flexible du système de mise à jour de tous les composants du réseau antivirus depuis SGM et diffusion de mises à jour sur les postes ; configuration de systèmes de notification de l'administrateur sur les événement du réseau antivirus avec les méthodes différentes d'envoi de notifications ; paramétrage des liaisons entre Serveurs pour configurer un réseau multi-serveurs.



Pour l'information détaillée sur les fonctionnalités décrites veuillez consulter **Manuel Administrateur**.

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 Le Centre de gestion Mobile supporte les fonctions de base du Centre de gestion :

1. Gestion des composants antivirus installés sur les postes du réseau antivirus :
 - lancement du scan rapide ou complet pour les postes sélectionnés ou pour tous les postes des groupes sélectionnés ;
 - configuration de la réaction du Scanner Dr.Web sur la détection d'objets malveillants ;
 - consultation et gestion des fichiers de la Quarantaine sur le poste sélectionné ou sur tous les postes du groupe sélectionné.
2. Affichage des statistiques sur le statut du réseau antivirus :



- nombre des postes enregistrés sur le Serveur Dr.Web et leur statut actuel (en ligne/hors ligne) ;
 - statistiques des infections sur les postes protégés.
3. Gestion des postes et des groupes :
 - consultation des paramètres ;
 - consultation et gestion du contenu des composants du package antivirus ;
 - suppression de postes et de groupes ;
 - envoi de messages sur les postes ;
 - redémarrage des postes tournant sous Windows ;
 - ajout des postes et des groupes aux favoris pour l'accès rapide.
 4. Consultation et gestion des messages sur les événements majeurs dans le réseau antivirus via les notifications interactives Push :
 - affichage de toutes les notifications sur le Serveur Dr.Web ;
 - spécification de la réaction sur les événements de notifications ;
 - recherche des notifications par paramètres spécifiés du filtre ;
 - suppression des notifications ;
 - prévention de la perte de notifications suite à une suppression automatique.
 5. Gestion des nouveaux postes qui attendent la connexion au Serveur Dr.Web :
 - approbation de l'accès ;
 - rejet des postes.
 6. La gestion des postes sur lesquels la mise à jour du logiciel antivirus a échoué :
 - affichage des postes échoués ;
 - mise à jour des composants sur les postes échoués.
 7. Gestion du référentiel du Serveur Dr.Web :
 - consulter le statut des produits dans le référentiel ;
 - lancer la mise à jour du référentiel depuis le Système Global de Mises à jour Dr.Web.
 8. Recherche des postes et des groupes sur le réseau antivirus par le nom, l'adresse ou l'ID.

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 systèmes 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.

En fonction du système d'exploitation du poste les fonctions suivantes sont fournies.

Postes tournant sous Windows

Protection antivirus

Scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion, y compris le scan anti-rootkits.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur de courrier

Analyse de tous les e-mails entrants et sortants en cas de l'utilisation de clients de messagerie.

Possibilité d'utiliser un filtre antispam (à condition que cette option soit autorisée par la licence).

Moniteur web

Analyse de toutes les requêtes vers les sites Web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple, dans les fichiers reçus/envoyés). Limitation de l'accès aux ressources suspectes ou incorrectes.

Office Control

Gestion de l'accès aux ressources réseau ou aux ressources locales, notamment, il contrôle l'accès aux sites web. Le composant permet non seulement de contrôler l'intégrité des fichiers importants qu'il protège contre toute modification occasionnelle ou infection virale, mais il bloque aussi l'accès des employés aux informations non sollicitées.



Pare-feu

Protection de l'ordinateur contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via Internet. Contrôle de la connexion et de la transmission de données via Internet et blocage de connexions suspectes au niveau de paquets et d'applications.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Autoprotection

Protection des fichiers et des dossiers de Dr.Web Enterprise Security Suite contre une suppression non autorisée ou involontaire ainsi que contre une modification par l'utilisateur ou par un malware. Lorsque l'autoprotection est active, seuls les processus Dr.Web ont accès aux fichiers et des dossiers de Dr.Web Enterprise Security Suite.

Protection préventive

Prévention de menaces potentielles à la sécurité. Contrôle d'accès aux objets critique du système d'exploitation, contrôle de téléchargement de pilotes, contrôle de démarrage automatique de programmes et de fonctionnement de services système. Surveillance de processus lancés et leur blocage en cas de détection d'une activité malveillante.

Contrôle des applications

Il surveille l'activité de tous les processus sur les postes. Il permet à l'administrateur du réseau antivirus de spécifier les applications dont le lancement sera autorisé ou bloqué sur les postes protégés.

Postes tournant sous l'OS de la famille UNIX

Protection antivirus

Moteur de scan. Il effectue l'analyse des données (contenu des fichiers, enregistrements de démarrage des périphériques de disques et autres données reçues des autres composants de Dr.Web pour UNIX). Il crée une file d'attente de l'analyse. Il désinfecte les menaces curables.

Analyse antivirus, gestion de la quarantaine

Composant de l'analyse des objets du système de fichiers et gestionnaire de la quarantaine. Il reçoit les tâches d'analyse de fichiers des autres composants de Dr.Web pour UNIX. Il contourne les répertoires du système de fichiers conformément à la tâche. il envoi des fichiers pour l'analyse du moteur de scan. Il supprime les fichiers infectés, les déplace en quarantaine, les restaure de la quarantaine et gère les répertoires de la quarantaine. Il organise et tient à jour le cache stockant les informations sur les fichiers analysés précédemment et le registre de menaces détectées.

Il est utilisé par tous les composants analysant les objets du système de fichiers, tel que SpIDer Guard (pour Linux, SMB, NSS).



Analyse du trafic web

Serveur ICAP exécutant l'analyse de requêtes et du trafic passant par les serveurs proxy HTTP. Il empêche le transfert des fichiers infectés et l'accès aux hôtes du réseau listés dans les catégories indésirables de ressources web et les listes noires créées par l'administrateur système.

Moniteur de fichiers pour les systèmes GNU/Linux

Moniteur du système de fichiers Linux. Il fonctionne en tâche de fond et suit les opérations avec les fichiers (telles que la création, l'ouverture, la fermeture et le lancement du fichier) dans les système de fichiers GNU/Linux. Il envoie au composant de l'analyse de fichiers les requêtes pour l'analyse du contenu de nouveaux fichiers et de fichiers modifiés, ainsi que des fichiers exécutables au moment du lancement de programmes.

Moniteur de fichiers pour les répertoires Samba

Moniteur des répertoires partagés Samba. Il fonctionne en tâche de fond et suit les opérations du système de fichiers (telles que la création, l'ouverture, la fermeture du fichier et les opérations de lecture et écriture) dans les répertoires servant des stockages de fichiers du serveur SMB de Samba. Il envoie au composant de l'analyse de fichiers le contenu de nouveaux fichiers et de fichiers modifiés.

Moniteur de fichiers NSS

Moniteur des volumes NSS (Novell Storage Services). Il fonctionne en tâche de fond et suit les opérations du système de fichiers (telles que la création, l'ouverture, la fermeture du fichier et les opérations d'écriture) sur les volumes NSS créés dans le point indiqué du système de fichiers. Il envoie au composant de l'analyse de fichiers le contenu de nouveaux fichiers et de fichiers modifiés.

Analyse des connexions réseau

Composant de l'analyse du trafic réseau d'URL. Il est conçu pour analyser pour la présence de menaces les données téléchargées depuis le réseau sur un hôte local et transmises de cet hôte dans le réseau externe. Il sert à empêcher la connexion avec les hôtes de réseau qui sont inscrits dans les catégories indésirables de ressources web ou bien, dans des listes noires créées par l'administrateur du réseau.

Moniteur de courrier

Composant de l'analyse des messages e-mail. Il analyse les messages des protocoles, trie les messages e-mail et les prépare à l'analyse pour la présence de menaces. Il peut fonctionner en deux modes :

1. Filtre pour les serveurs de messagerie (Sendmail, Postfix, etc), connecté via l'interface Milter, Spamd ou Rspamd.
2. Proxy transparent de protocoles de messagerie (SMTP, POP3, IMAP). Dans ce mode, il utilise SpIDer Gate.



Postes tournant sous macOS

Protection antivirus

Le scan de l'ordinateur selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Analyse de tous les processus lancés ainsi que des fichiers créés sur les disques durs et des fichiers ouverts sur les supports amovibles.

Moniteur web

Analyse de toutes les requêtes vers les sites web via le protocole HTTP. Neutralisation des menaces contenues dans le trafic HTTP (par exemple dans les fichiers reçus/envoyés). Blocage de l'accès aux ressources suspectes ou incorrectes.

Quarantaine

Isolation des objets malveillants ou suspects dans un répertoire spécial.

Appareils mobiles tournant sous OS Android

Protection antivirus

Le scan de l'appareil mobile selon la requête de l'utilisateur et selon la planification. Il est également possible de lancer sur les postes le scan antivirus à distance depuis le Centre de gestion.

Moniteur de fichiers

Analyse permanente à la volée du système de fichiers. Scan de tous les fichiers lors de la tentative de sauvegarder ces fichiers dans la mémoire de l'appareil mobile.

Filtre des appels et des SMS

Le filtrage des appels et des messages SMS permet de bloquer des messages et des appels indésirables, par exemple, des messages publicitaires ou des appels et des messages de numéros inconnus.

Antivol

Détection de l'appareil mobile ou le blocage rapide de fonctionnalités en cas de perte ou de vol.

Restriction de l'accès aux ressources web

Le filtre URL permet de protéger l'utilisateur de l'appareil mobile contre les ressources web indésirables.



Pare-feu

Protection de l'appareil mobile contre tout accès non autorisé de l'extérieur ainsi que contre des fuites de données importantes via le réseau. Contrôle de la connexion et de la transmission de données via Internet et blocage de connexions suspectes au niveau de paquets et d'applications.

Aide dans la résolution de problèmes de sécurité

Diagnostic et analyse de sécurité de l'appareil mobile et résolution de problèmes et de vulnérabilités détectés.

Contrôle de lancement des applications

Interdiction de lancer sur l'appareil mobile des applications qui ne sont pas incluses dans la liste des applications autorisées par l'administrateur.

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.

Le Serveur proxy permet d'utiliser tout ordinateur faisant partie du réseau antivirus dans les buts suivants :

- Comme le centre de retransmission des mises à jour pour réduire la charge réseau sur le Serveur Dr.Web et la connexion entre le Serveur Dr.Web et le Serveur proxy et pour réduire le délai de réception de mises à jour par les postes grâce à l'utilisation de la fonction de mise en cache.
- Comme le centre de transmission des événements viraux des postes protégés vers le Serveur Dr.Web, ce qui aussi réduit la charge système et permet de gérer les cas où, par exemple, le groupe de postes se trouve dans le segment isolé du segment dans lequel se trouve le Serveur Dr.Web.

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. Le niveau de sécurité est assuré grâce à la capacité de répondre aux exigences opérationnelles relatives aux systèmes dans le réseau.

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



Numéros de ports	Protocoles	Connexions	Usage
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		Pour le fonctionnement de l'utilitaire de diagnostic distant du Serveur Dr.Web
10101	TCP		
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) :



Paramètre	Configuration requise
	<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.	<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,



Windows	UNIX
<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">▪ 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.
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	<p>Un des navigateurs suivants :</p> <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,



	<ul style="list-style-type: none">• Opera en dernière version,• Safari en dernière version,• Yandex Browser en dernière version
Résolution de l'écran	Résolution de l'écran recommandée — 1280x1024
Autre	<p>En cas d'utilisation du navigateur web Windows Internet Explorer, il faut prendre en compte les particularités suivantes :</p> <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



Paramètre	Configuration requise
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
Système d'exploitation	Pour les systèmes d'exploitation 32 bits : <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. Pour les systèmes d'exploitation 64 bits : <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 ;



Paramètre	Pré-requis
	<ul style="list-style-type: none">• 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	Le programme fonctionne dans les environnements suivants : <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 ;• Outlook 2002 ;• Outlook 2003 ;• Outlook 2007 ;• Outlook 2010 avec SP2 ;• Outlook 2013 ;• Outlook 2016 ;• Outlook 2019 ;• Outlook 2021

UNIX

Composant	Pré-requis
Plateforme	<p>Les processeurs avec les architectures et les systèmes de commandes suivants sont pris en charge :</p> <ul style="list-style-type: none">• Intel/AMD : 32 bits (IA-32, x86) ; 64 bits (x86-64, x64, amd64) ;• ARM64 ;



Composant	Pré-requis
	<ul style="list-style-type: none">• 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	<p>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.</p> <p>Le système d'exploitation doit prendre en charge le mécanisme d'authentification PAM</p>
Autre	<p>Les connexions réseau suivantes sont requises :</p> <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), 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



Plateforme	Versions GNU/Linux prises en charge
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 ;



Paramètre	Configuration requise
	<ul style="list-style-type: none">• 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 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 ;



Paramètre	Pré-requis
	<ul style="list-style-type: none">• 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
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,



Paramètre	Pré-requis
	<ul style="list-style-type: none">• IBM Notes pour Windows 10.0,• HCL Domino pour Windows 11.0,• HCL Notes pour Windows 11.0. <p>Navigateurs pour la gestion de l'interface web :</p> <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`

Installeur 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 : 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 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](#).



Chapitre 4 : Mise en route

4.1. 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 les 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 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 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 , 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 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 la 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 composants 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 les 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](#)).

4.2. Configuration des connexions réseau

Généralités

Les client suivants se connectent au Serveur Dr.Web :

- Agents Dr.Web.
- Installateurs des Agents Dr.Web.
- Les Serveurs voisins Dr.Web.
- Serveurs proxy Dr.Web.

La connexion est toujours initiée par le client.

Les schémas suivants de connexion au Serveur Dr.Web sont disponibles :

1. Via les [connexions directes](#).

Cette approche présente certains avantages mais il n'est pas toujours recommandé de l'utiliser.

2. En utilisant le [Service de détection de Serveur Dr.Web](#).

Par défaut (si une autre configuration n'est pas spécifiée), les clients utilisent ce Service.



Cette approche est recommandée dans le cas où une reconfiguration de tout le système est nécessaire et notamment s'il faut déplacer le Serveur Dr.Web vers un autre ordinateur ou changer d'adresse IP de l'ordinateur sur lequel est installé le Serveur Dr.Web.

3. Via le [protocole SRV](#).

Cette approche permet de rechercher un Serveur Dr.Web par le nom d'un ordinateur ou le service de Serveur Dr.Web via les enregistrements SRV sur le serveur DNS.

Si le réseau antivirus Dr.Web Enterprise Security Suite est configuré pour utiliser les connexions directes, le Service de détection de Serveur Dr.Web peut être désactivé. Pour cela, dans la partie transport, laissez vide le champ **Groupe Multicast** (**Administration** → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet **Transport**).

Configuration du pare-feu

Afin d'assurer l'interaction entre les composants du réseau antivirus, il est nécessaire que tous les ports et interfaces utilisés soient ouverts sur tous les postes se trouvant dans le réseau antivirus.

Lors de l'installation du Serveur Dr.Web, l'installateur ajoute automatiquement les ports et les interfaces du Serveurs Dr.Web dans les exceptions du pare-feu Windows.

En cas d'utilisation d'un autre pare-feu que celui de Windows, l'administrateur du réseau antivirus doit configurer manuellement les paramètres concernés.

4.2.1. Connexions directes

Configuration du Serveur Dr.Web

L'adresse qu'il faut écouter pour la réception de connexions TCP entrantes doit être indiquée dans les paramètres du Serveur Dr.Web (voir le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#)).

Vous pouvez configurer ce paramètre dans la configuration du Serveur Dr.Web :

Administration → **Configuration du Serveur Dr.Web** → onglet **Réseau** → onglet **Transport** → champ **Adresse**.

Les paramètres suivants sont définis par défaut pour l'écoute par le Serveur Dr.Web :

- **Adresse** : valeur vide — utiliser *toutes les interfaces réseau* pour cet ordinateur sur lequel le Serveur Dr.Web est installé.
- **Port** : 2193 — utiliser le port 2193.



Le port 2193 est enregistré pour Dr.Web Enterprise Management Service dans IANA.



Pour assurer le fonctionnement correct du réseau antivirus Dr.Web Enterprise Security Suite, il suffit que le Serveur Dr.Web « soit à l'écoute » d'au moins un port TCP qui doit être connu de tous les clients.

Configuration de l'Agent Dr.Web

Lors de l'installation de l'Agent Dr.Web, l'adresse du Serveur Dr.Web (l'adresse IP, NetBIOS ou le nom de domaine de l'ordinateur sur lequel le Serveur Dr.Web est lancé) peut être indiquée directement dans les paramètres d'installation :

```
drwinst /server <Adresse_du_Serveur_Dr.Web>
```

Lors de l'installation de l'Agent Dr.Web, il est recommandé d'utiliser le nom du Serveur Dr.Web au format FQDN en tant qu'adresse du Serveur Dr.Web au [format FQDN](#). Cela facilitera le processus de configuration du réseau antivirus relatif à la procédure de réinstallation du Serveur Dr.Web sur un autre ordinateur. Dans ce cas, si vous voulez changer l'adresse du Serveur Dr.Web, il suffira de la changer dans les paramètres du serveur DNS pour le nom de l'ordinateur hébergeant le Serveur Dr.Web. Tous les agents se connecteront automatiquement au nouveau serveur.

Par défaut, la commande `drwinst`, lancée sans paramètres, va scanner le réseau pour rechercher les Serveurs Dr.Web et tenter d'installer l'Agent Dr.Web depuis le premier Serveur Dr.Web trouvé dans le réseau (mode *Multicasting* utilisant le [Service de détection de Serveur Dr.Web](#)).

Ainsi, l'adresse du Serveur Dr.Web est connue par l'Agent Dr.Web lors de l'installation.

Ultérieurement, l'adresse du Serveur Dr.Web peut être modifiée manuellement dans les paramètres de l'Agent Dr.Web.

4.2.2. Service de détection du Serveur Dr.Web

En cas de connexion selon ce schéma, le client ne connaît pas d'avance l'adresse du Serveur Dr.Web. Avant d'établir chaque connexion, une recherche du Serveur Dr.Web dans le réseau sera effectuée. Pour cela, le client envoie une requête broadcast et attend une réponse contenant l'adresse du Serveur Dr.Web. Dès que la réponse est réceptionnée, le client établit une connexion au Serveur Dr.Web.

Pour cela, le Serveur Dr.Web doit "écouter" le réseau pour réceptionner de telles requêtes.

Plusieurs variantes de configuration de ce schéma sont possibles. Il est important que la méthode de recherche du Serveur Dr.Web configurée pour les clients corresponde à la configuration de réponse du Serveur Dr.Web.

Dr.Web Enterprise Security Suite utilise par défaut le mode *Multicast over UDP* :

1. Le Serveur Dr.Web s'enregistre dans le groupe multicast avec une adresse spécifiée dans les paramètres du Serveur Dr.Web.



2. Les Agents Dr.Web lorsqu'ils recherchent le Serveur Dr.Web, envoient des requêtes multicast à l'adresse de groupe spécifiée à l'étape 1.

Le Serveur Dr.Web écoute par défaut l'adresse `udp/231.0.0.1:2193` (idem pour les connexions directes).

Ce paramètre est spécifié dans les paramètres du Centre de gestion **Administration** → **Configuration du Serveur Dr.Web** → **Réseau** → **Transport** → **TCP/IP**. La valeur vide indique d'utiliser l'adresse par défaut indiquée ci-dessus.

4.2.3. Utiliser le protocole SRV

Les clients sous Windows supportent le protocole réseau client *SRV* (une description du format est donnée dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#)).

L'accès au Serveur Dr.Web via les enregistrements SRV est implémenté de la façon suivante :

1. Durant l'installation du Serveur Dr.Web, l'enregistrement dans le domaine Active Directory est paramétré, les registres d'installation correspondant à l'enregistrement SRV sur le serveur DNS.



L'enregistrement SRV est inscrit sur le serveur DNS selon RFC2782 (voir <https://datatracker.ietf.org/doc/html/rfc2782>).

2. Dans une requête pour la connexion au Serveur Dr.Web, le client spécifie que l'accès a lieu via le protocole *srv*.

Par exemple, le lancement de l'installateur de l'Agent Dr.Web :

- avec mention explicite du nom du service *myservice* :
`drwinst /server "srv/myservice"`
- sans mention du nom du service. Dans ce cas, le nom par défaut *drwcs* sera recherché dans les entrées SRV :
`drwinst /server "srv/"`

3. De manière transparente pour l'utilisateur, le client utilise le protocole SRV pour accéder au Serveur Dr.Web.



Si le Serveur Dr.Web n'est pas indiqué directement, la commande *drwcs* est utilisée par défaut comme nom du service.



4.3. Assurance d'une connexion sécurisée

4.3.1. Chiffrement et compression du trafic

Le mode de chiffrement est utilisé pour assurer la protection des données transmises par un canal non sécurisé et permet d'éviter la divulgation des données importantes et la substitution des logiciels téléchargés sur les postes protégés.

Le réseau antivirus Dr.Web Enterprise Security Suite utilise les outils cryptographiques suivants :

- Signature numérique (GOST R 34.10-2001).
- Chiffrement asymétrique (VKO GOST R 34.10-2001 – RFC 4357).
- Chiffrement symétrique (GOST 28147-89).
- Fonction de hachage cryptographique (GOST R 34.11-94).

Le réseau antivirus Dr.Web Enterprise Security Suite permet de chiffrer le trafic entre le Serveur Dr.Web et les clients qui comprennent:

- Agents Dr.Web.
- Installateurs des Agents Dr.Web.
- Les Serveurs voisins Dr.Web.
- Les Serveurs proxy Dr.Web.

Compte tenu du fait que le trafic entre les composants (surtout entre les Serveurs Dr.Web) peut être assez important, le réseau antivirus permet de compresser le trafic. La politique de compression et la compatibilité des paramètres des divers clients sont équivalents aux paramètres de chiffrement.

Politique de concordance des paramètres

La politique de chiffrement et de compression peut être configurée séparément sur chaque composant du réseau antivirus, la configuration d'autres composants doit être conforme à celle du Serveur Dr.Web.

Pour assurer une concordance entre les politiques de chiffrement et de compression sur le Serveur Dr.Web et sur un client, il faut noter qu'il existe des paramètres incompatibles dont la sélection entraîne l'échec de connexion entre le Serveur Dr.Web et le client concerné.

Le [tableau 4-1](#) comprend les combinaisons des paramètres qui assurent (+) ou n'assurent pas (-) le chiffrement et la compression de la connexion entre le Serveur Dr.Web et le client ainsi que les combinaisons inappropriées (**Erreur**).

**Tableau 4-1. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression**

Paramètres de client	Paramètres du Serveur Dr.Web		
	Oui	Possible	Non
Oui	+	+	Erreur
Possible	+	+	-
Non	Erreur	-	-



Le chiffrement du trafic entraîne une charge importante sur les ordinateurs dont les performances sont proches de la limite inférieure des pré-requis relatifs aux composants installés. Dans le cas où le chiffrement du trafic n'est pas indispensable pour la sécurité, il est possible de ne pas l'utiliser.

Pour désactiver le mode de chiffrement, il faut d'abord basculer les paramètres du Serveur Dr.Web et des composants vers le statut **Possible** afin d'éviter l'apparition de paires de paramètres incompatibles client-serveur.

L'utilisation de la compression diminue le trafic mais augmente considérablement l'utilisation de la mémoire vive et la charge sur les ordinateurs, beaucoup plus que le chiffrement.

Connexion via le Serveur proxy Dr.Web

Lors de la connexion des clients au Serveur Dr.Web via le Serveur proxy Dr.Web, il faut tenir compte des paramètres de chiffrement et de compression de tous les trois composants. Dans ce cas :

- Les paramètres du Serveur Dr.Web et du Serveur proxy (ici, il sert du client) doivent être coordonnés selon [le tableau 4-1](#).
- Les paramètres du client et du Serveur proxy (ici, il sert du Serveur Dr.Web) doivent être coordonnés selon [le tableau 4-1](#).

La possibilité de connexion via le Serveur proxy dépend de la version du Serveur Dr.Web et celle du client supportant des technologies de chiffrement particulières :

- Si le Serveur Dr.Web et le client supportent le chiffrement TLS utilisé dans la version 13.0, il suffit de satisfaire aux [conditions décrites ci-dessus](#) pour établir une connexion fonctionnelle.
- Si un des composants ne supporte pas le chiffrement TLS : la version 10 ou une version antérieure avec le chiffrement selon GOST est installée sur le Serveur Dr.Web et/ou le client, une vérification supplémentaire selon [le tableau 4-2](#) est effectuée.

**Tableau 4-2. Compatibilité des paramètres relatifs aux politiques de chiffrement et de compression en cas d'utilisation du Serveur proxy**

Paramètres de connexion avec le client	Paramètres de connexion avec le Serveur Dr.Web			
	Rien	Compression	Chiffrement	Tout
Rien	Mode standard	Mode standard	Erreur	Erreur
Compression	Mode standard	Mode standard	Erreur	Erreur
Chiffrement	Erreur	Erreur	Mode transparent	Erreur
Tout	Erreur	Erreur	Erreur	Mode transparent

Conventions

Paramètres de connexion avec le Serveur Dr.Web et le client	
Rien	Ni la compression, ni le chiffrement n'est supporté.
Compression	Seule la compression est supportée.
Chiffrement	Seul le chiffrement est supporté.
Tout	La compression et le chiffrement sont supportés.

Résultat de la connexion	
Mode standard	La connexion établie signifie le fonctionnement en mode standard avec le traitement de commandes et la mise en cache.
Mode transparent	La connexion établie signifie le fonctionnement en mode transparent : sans traitement de commandes et la mise en cache. Le version sélectionnée du protocole de chiffrement est minimale : si un des composants (Serveur Dr.Web ou Agent Dr.Web) est en version 13, et l'autre — en version 10, le chiffrement utilisé dans la version 10 sera spécifié.
Erreur	La connexion du Serveur proxy avec le Serveur Dr.Web et le client sera interrompue.

Ainsi, si le Serveur Dr.Web et l'Agent Dr.Web sont en versions différentes : l'un est en version 13. L'autre — en version 10 ou antérieure, les restrictions suivantes sont appliquées pour les connexions établies via le Serveur proxy :

- La mise en cache des données du Serveur proxy est possible uniquement si les deux connexions — avec le Serveur Dr.Web et avec le client sont établies sans l'utilisation de chiffrement.



- Le chiffrement sera utilisé uniquement si les deux connexions avec le Serveur Dr.Web et le client sont établies avec l'utilisation de chiffrement et les mêmes paramètres de compression (la compression est utilisée ou n'est pas utilisée pour les deux connexions).

Paramètres de chiffrement et de compression sur le Serveur Dr.Web

Pour configurer les paramètres de compression et de chiffrement du Serveur Dr.Web

1. Sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion.
2. Dans la fenêtre qui s'affiche, sélectionnez l'élément du menu de gestion **Configuration de Serveur Dr.Web**.
3. Dans l'onglet **Réseau** → **Transport**, sélectionnez dans les listes déroulantes **Chiffrement** et **Compression** l'une des variantes suivantes :
 - **Oui** : le chiffrement (ou la compression) du trafic entre tous les clients est obligatoire (la valeur est spécifiée par défaut pour le chiffrement, si le paramètre n'a pas été modifié lors de l'installation du Serveur Dr.Web).
 - **Possible** : le chiffrement (ou la compression) sera appliqué au trafic relatif aux clients dont les paramètres le permettent.
 - **Non** : le chiffrement (ou la compression) n'est pas supporté (la valeur est spécifiée par défaut pour la compression si le paramètre n'a pas été modifié lors de l'installation du Serveur Dr.Web).



Quand vous configurez le chiffrement et la compression du côté du Serveur Dr.Web, prenez en compte les particularités de clients que vous projetez de connecter à ce Serveur Dr.Web. Pas tous les clients supportent le chiffrement et la compression du trafic.

Paramètres de chiffrement et de compression sur le Serveur proxy Dr.Web

Pour configurer de manière centralisée les paramètres de chiffrement et de compression pour le Serveur proxy




Si le Serveur proxy n'est pas connecté au Serveur Dr.Web, pour pouvoir gérer les paramètres à distance, configurez la connexion, comme cela est décrit dans le p. [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#).

1. Ouvrez le Centre de gestion pour le Serveur Dr.Web qui gère le Serveur proxy.
2. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, dans la liste hiérarchique, cliquez sur le nom du Serveur proxy



dont vous voulez éditer les paramètres ou sur le nom de son groupe primaire si les paramètres du Serveur proxy sont hérités.

3. Dans le menu de gestion qui s'affiche, sélectionnez l'élément **Serveur proxy Dr.Web**. La section des paramètres va s'ouvrir.
4. Ouvrez l'onglet **Écoute**.
5. Dans la liste déroulante **Paramètres de connexion avec les clients**, dans les listes déroulantes **Chiffrement** et **Compression**, sélectionnez le mode de chiffrement et de compression du trafic pour les canaux entre le Serveur proxy et les clients servis : les Agents Dr.Web et les installateurs des Agents Dr.Web.
6. Dans la section **Paramètres de connexion avec les Serveurs Dr.Web**, la liste des Serveurs vers lesquels le trafic sera redirigé est spécifiée. Sélectionnez le Serveur Dr.Web nécessaire dans la liste et cliquez sur le bouton  dans la barre d'outils de cette section pour modifier les paramètres de connexion au Serveur Dr.Web sélectionné. Dans la fenêtre qui s'affiche, dans les listes déroulantes **Chiffrement** et **Compression**, sélectionnez le mode de chiffrement et de compression du trafic pour le canal entre le Serveur proxy et le Serveur Dr.Web sélectionné.
7. Pour sauvegarder les paramètres spécifiés, cliquez sur **Enregistrer**.

Pour configurer de manière locale les paramètres de chiffrement et de compression pour le Serveur proxy



Si le Serveur proxy est connecté au Serveur Dr.Web gérant pour la configuration à distance, le fichier de configuration du Serveur proxy sera réécrit conformément aux paramètres reçus du Serveur Dr.Web. Dans ce cas, il faut spécifier les paramètres à distance depuis le Serveur Dr.Web ou désactiver les paramètres autorisant d'accepter la configuration de ce Serveur Dr.Web.

Le fichier de configuration `drwcsd-proxy.conf` est décrit dans les **Annexes**, [F4. Fichier de configuration du Serveur proxy Dr.Web](#).

1. Ouvrez le fichier de configuration `drwcsd-proxy.conf` sur l'ordinateur, sur lequel le Serveur proxy est installé.
2. Éditez les paramètres responsables de compression et de chiffrement pour les connexions avec les clients et les Serveurs Dr.Web.
3. Redémarrez le Serveur proxy :
 - Sous Windows :
 - Si le Serveur proxy est lancé en tant que service de l'OS Windows, le redémarrage s'effectue avec des outils standard du système.
 - Si le Serveur proxy est lancé dans la console, cliquez sur CTRL+BREAK pour le redémarrer.
 - Pour les OS de la famille UNIX :
 - Envoyez le signal `SIGHUP` au daemon du Serveur proxy.



- Exécutez la commande suivante :

Sous Linux :

```
/etc/init.d/dwcp_proxy restart
```

Sous FreeBSD :

```
/usr/local/etc/rc.d/dwcp_proxy restart
```

Paramètres de chiffrement et de compression sur les postes

Pour configurer de manière centralisée les paramètres de chiffrement et de compression sur les postes.

1. Sélectionnez l'élément **Réseau antivirus** dans le menu principal du Centre de gestion, puis dans la fenêtre qui apparaît, cliquez sur le nom du poste ou du groupe dans l'arborescence.
2. Dans le menu de gestion qui s'affiche, sélectionnez l'élément **Paramètres de connexion**.
3. Dans l'onglet **Général**, sélectionnez dans les listes déroulantes **Mode de chiffrement** et **Mode de compression** l'une des variantes suivantes :
 - **Oui** : le chiffrement (ou la compression) du trafic avec le Serveur Dr.Web est obligatoire.
 - **Possible** : le chiffrement (ou la compression) sera appliqué au trafic avec le Serveur Dr.Web, si les paramètres du Serveur Dr.Web le permettent.
 - **Non** : le chiffrement (ou la compression) n'est pas supporté.
4. Cliquez sur **Enregistrer**.
5. Les modifications seront appliquées dès que les paramètres auront été transmis sur les postes. Si les postes sont désactivés au moment de la modification des paramètres, les modifications seront transmises sur les postes juste après leur connexion au Serveur Dr.Web.

Agent Dr.Web pour Windows

Les paramètres de chiffrement et de compression peuvent être spécifiés lors de l'installation de l'Agent :

- En cas d'installation distante depuis le Centre de gestion, le mode de chiffrement et de compression est spécifié directement dans les paramètres de la section **Installation via le réseau**.
- En cas d'installation locale, l'installateur graphique n'accorde pas la possibilité de modifier le mode de chiffrement et de compression, pourtant ces paramètres peuvent être spécifiés à l'aide des clés de la ligne de commande lors du lancement de l'installateur (voir le document **Annexes, [G1. Installateur réseau](#)**).

Après l'installation de l'Agent Dr.Web, la possibilité de modifier les paramètres de chiffrement ou de compression sur le poste de manière locale n'est pas accordée. Le mode **Possible** est spécifié par défaut (si une autre valeur n'a pas été spécifiée), cela veut dire que l'utilisation du



chiffrement et de la compression dépend des paramètres du côté du Serveur Dr.Web. Pourtant les paramètres du côté de l'Agent Dr.Web peuvent être modifiés via le Centre de gestion (voir [ci-dessus](#)).

Antivirus Dr.Web pour Android

L'Antivirus Dr.Web pour Android ne supporte ni chiffrement, ni compression. La connexion est impossible si la valeur **Oui** est spécifiée pour le chiffrement et/ou la compression du côté du Serveur Dr.Web ou du Serveur proxy (en cas de connexion via le Serveur proxy).

Antivirus Dr.Web pour Linux

Lors de l'installation de l'antivirus le mode de chiffrement et de compression ne peut pas être modifié. Le mode **Possible** est spécifié par défaut.

Après l'installation de l'antivirus, vous avez la possibilité de modifier les paramètres de chiffrement et de compression sur le poste uniquement en mode de la ligne de commande. Pour en savoir plus sur ce mode et les clés correspondantes de la ligne de commande, consultez le **Manuel utilisateur Dr.Web pour Linux**.

Les paramètres peuvent également être spécifiés du côté du poste via le Centre de gestion (voir [ci-dessus](#)).

Antivirus Dr.Web pour macOS

La possibilité de modifier les paramètres de chiffrement ou de compression sur le poste de manière locale n'est pas accordée. Le mode **Possible** est spécifié par défaut, cela veut dire que l'utilisation du chiffrement et de la compression dépend des paramètres de côté du Serveur Dr.Web.

Les paramètres du côté du poste peuvent être modifiés via le Centre de gestion (voir [ci-dessus](#)).

4.3.2. Instruments assurant une connexion sécurisée

Lors de l'installation du Serveur Dr.Web, les outils suivants sont créés assurant la connexion sécurisées entre les composants du réseau antivirus :

1. Clé privée de chiffrement du Serveur Dr.Web`drwcsd.pri`.

Sauvegardée sur le Serveur Dr.Web et n'est pas transmise aux autres composants du réseau antivirus.

Si la clé privée est perdue, il faut rétablir manuellement la connexion entre les composants du réseau antivirus (créer tous les clés et les certificats et les distribuer sur tous les composants du réseau antivirus).



La clé privée est utilisée dans les cas suivants :

a) *Création des clés publiques et des certificats.*

La clé de chiffrement publique et le certificat sont créés automatiquement de la clé privée lors de l'installation du Serveur Dr.Web. Dans ce cas, une nouvelle clé privée peut être créée ou bien la clé existante (de la dernière installation du Serveur Dr.Web) peut être utilisée. Les clés de chiffrement et les certificats peuvent être créés à tout moment à l'aide de l'utilitaire de serveur `drwsign` (voir le document **Annexes**, [H7.1. Utilitaire de génération des clés et des certificats](#)).

Vous trouverez les informations sur les clés publiques et les certificats ci-dessous.

b) *Authentification du Serveur Dr.Web.*

L'authentification du Serveur Dr.Web par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).

Le Serveur Dr.Web effectue la signature numérique du message avec la clé privée et envoie le message au client. Le client vérifie la signature du message à l'aide du certificat.

c) *Déchiffrement des données.*

En cas de chiffrement du trafic entre le Serveur Dr.Web et les clients, les données envoyées par le client sont déchiffrées sur le Serveur Dr.Web avec la clé publique.

2. Clé publique de chiffrement du Serveur Dr.Web *.pub.

Disponible pour tous les composants du réseau antivirus. La clé publique peut toujours être générée de la clé privée (voir [ci-dessus](#)). A chaque génération depuis la même clé privée, vous obtenez la même clé publique.

A partir de la version 11 du Serveur Dr.Web, la clé publique est utilisée pour la communication avec les clients des versions précédentes. Les autres fonctions sont transférées au certificat qui en même temps contient la clé publique de chiffrement.

3. Certificat du Serveur Dr.Web `drwcsd-certificate.pem`.

Disponible pour tous les composants du réseau antivirus. Le certificat contient la clé publique de chiffrement. Le certificat peut être généré de la clé privée (voir [ci-dessus](#)). A chaque génération depuis la même clé privée, vous obtenez un nouveau certificat.

Les clients connectés au Serveurs Dr.Web sont rattaché à un certificat particulier, c'est pourquoi en cas de perte du certificat sur le client vous pourrez le restaurer uniquement au cas où le même certificat est utilisé par un autre composant réseau : dans ce cas on peut copier sur le client depuis le Serveur Dr.Web ou depuis un autre client.

La certificat est utilisé dans les cas suivants :

a) *Authentification du Serveur Dr.Web.*

L'authentification du Serveur Dr.Web par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).



Le Serveur Dr.Web effectue la signature numérique du message avec la clé privée et envoie le message au client. Le client vérifie la signature du message à l'aide du certificat (notamment, à l'aide de la clé publique indiquée dans le certificat). Dans les versions précédentes du Serveur Dr.Web, c'était la clé publique qui était utilisée à cet effet.

Pour cela, il faut qu'un ou plusieurs certificats fiables des Serveurs Dr.Web auxquels le client peut se connecter soient disponibles sur le client.

b) Chiffrement des données.

En cas de chiffrement du trafic entre le Serveur Dr.Web et les Clients, les données sont chiffrées par le client avec la clé publique.

c) Réalisation d'une session TLS entre le Serveur Dr.Web et les clients distants.

d) Authentification du Serveur proxy.

L'authentification des Serveurs proxy Dr.Web par les clients distants s'effectue à la base de la signature numérique (une fois pour chaque connexion).

Le Serveur proxy signe ses certificats par la clé privée et le certificat du Serveur Dr.Web. Le client qui fait confiance au certificat du Serveur Dr.Web aura confiance aux certificats qu'il a signés.

4. Clé privée de chiffrement du serveur web.

Sauvegardée sur le Serveur Dr.Web et n'est pas transmise aux autres composants du réseau antivirus. Pour plus d'informations, voir ci-dessous.

5. Certificat du serveur web.

Disponible pour tous les composants du réseau antivirus.

Utilisé pour réaliser une session TLS entre le serveur web et le navigateur (via HTTPS).

Lors de l'installation du Serveur Dr.Web à la base de la clé privée du serveur web, un certificat auto-signé est généré qui ne sera pas accepté par les navigateurs web car il n'a pas été délivré par un centre de certification connu.

Pour que la connexion sécurisée (HTTPS) soit disponible, effectuez l'une des actions suivantes :

- Ajouter le certificat auto-signé aux fiables ou aux exclusions pour tous les postes et les navigateurs sur lesquels le Centre de gestion est ouvert.
- Obtenir le certificat signé par le centre de certification connu.

4.3.3. Connexion des clients au Serveur Dr.Web

Pour pouvoir se connecter au Serveur Dr.Web le certificat du Serveur Dr.Web doit être présent du côté de client que le trafic entre le Serveur Dr.Web et le client soit chiffré ou non.

Les clients suivants peuvent se connecter au Serveur Dr.Web :



- **Agents Dr.Web.**

Pour le fonctionnement de l'Agent Dr.Web en mode centralisé avec la connexion au Serveur Dr.Web, il faut qu'un ou plusieurs certificats fiables des Serveurs Dr.Web auxquels l'Agent Dr.Web peut se connecter soient disponibles.

Le certificat utilisé lors de l'installation et les certificats reçus via les paramètres centralisés depuis le Serveur Dr.Web sont sauvegardés dans le registre, mais les fichiers de certificats ne sont pas utilisés.

Le fichier de certificat en seul exemplaire peut être ajouté à l'aide de la clé de la ligne de commande dans le répertoire de l'Agent Dr.Web (mais pas dans le registre) et la liste commune des certificats utilisés. Ce certificat sera utilisé pour la connexion au Serveur Dr.Web en cas d'erreur dans les paramètres centralisés.

Si le certificat est introuvable ou invalide, l'Agent Dr.Web ne pourra pas se connecter au Serveur Dr.Web, mais il continuera à fonctionner et effectuer les mises à jour en Mode mobile s'il est autorisé pour ce poste.

- **Installeurs des Agents Dr.Web.**

Lors de l'installation de l'Agent Dr.Web sur le poste, le certificat du Serveur Dr.Web doit être présent, tout comme le fichier d'installation sélectionné.

Si vous lancez le package d'installation créé dans le Centre de gestion, le certificat est inclus dans le package d'installation. Dans ce cas, il ne faut pas indiquer en outre le fichier de certificat.

Après l'installation de l'Agent Dr.Web, les données du certificat sont inscrit dans le registre, le fichier du certificat n'est plus utilisé.

Si le certificat est introuvable ou indisponible, l'installateur ne pourra pas installer l'Agent Dr.Web (cela concerne tous les types des fichiers d'installation de l'Agent Dr.Web).

- **Les Serveurs voisins Dr.Web.**

Si vous configurez les connexions entre les Serveurs voisins Dr.Web en version 11 ou supérieure, sur chaque Serveur Dr.Web configuré il vous faudra spécifier le certificat du Serveur Dr.Web avec lequel vous voulez établir la liaison (voir le **Manuel Administrateur**, le p. [Configuration des liaisons entre les Serveurs Dr.Web](#)).

Si au moins un certificat est introuvable ou invalide, l'établissement de la liaison entre serveurs sera impossible.

- **Serveurs proxy Dr.Web.**

Pour la connexion du Serveur proxy au Serveur Dr.Web avec la possibilité de la configuration distante via le Centre de gestion, il faut que le certificat soit présent sur le poste avec le Serveur proxy installé. Dans ce cas, le Serveur proxy pourra supporter le chiffrement.

Si le certificat est introuvable, le Serveur proxy continuera à fonctionner, mais la gestion à distance, le chiffrement et la mise en cache seront indisponibles.



En cas de mise à niveau standard de tout le réseau antivirus de la version précédente qui utilisait les clés publiques vers la nouvelle version qui utilise les certificats, aucune action supplémentaire n'est requise.

L'installation de l'Agent Dr.Web fourni avec le Serveur Dr.Web en version 11 avec la connexion au Serveur Dr.Web en version 10 et vice-versa n'est pas recommandée.

4.4. Intégration de Dr.Web Enterprise Security Suite avec Active Directory

Si le service Active Directory est utilisé dans le réseau local protégé, vous pouvez configurer l'intégration des composants de Dr.Web Enterprise Security Suite avec ce service.



Toutes les méthodes listées ci-dessous sont autonomes et elles peuvent être appliquées ensemble ou séparément.

L'intégration de Dr.Web Enterprise Security Suite avec Active Directory s'effectue à la base de méthodes suivantes :

1. L'enregistre, du Serveur Dr.Web dans le domaine Active Directory pour appeler le Serveur Dr.Web via le protocole SRV

Lors de l'installation du Serveur Dr.Web, vous avez la possibilité d'enregistrer le Serveur dans le domaine Active Directory via l'installateur. Lors de l'enregistrement sur le serveur DNS, l'enregistrement SRV correspondant au Serveur Dr.Web sera créé. Ensuite, les clients pourront accéder au Serveur Dr.Web via cet enregistrement SRV.

Pour en savoir plus, voir [Installation du Serveur Dr.Web sous Windows](#) et [Utilisation du protocole SRV](#).

2. Synchronisation de la structure du réseau antivirus avec le domaine Active Directory

Il existe une possibilité de synchroniser automatiquement les structures du réseau avec les postes du domaine Active Directory. Dans ce cas, les conteneurs Active Directory qui contiennent des ordinateurs deviennent des groupes du réseau antivirus dans lesquels les postes de travail sont placés.

Pour cela, la tâche **Synchronisation avec Active Directory** est fournie dans la planification du Serveur Dr.Web. L'administrateur doit créer cette tâche lui-même ou avec le Planificateur de tâches du Serveur Dr.Web.

Pour en savoir plus, consultez le **Manuel Administrateur** [Configuration de la planification du Serveur Dr.Web](#).



3. Authentification des utilisateurs d'Active Directory sur le Serveur Dr.Web en tant qu'administrateurs

Il existe une possibilité d'authentifier sur le Serveur Dr.Web les utilisateurs sous les comptes d'Active Directory pour la gestion du réseau antivirus. Pour ce faire, il faut utiliser l'un des moyens suivants :

- Authentification LDAP/AD. Disponible pour les Serveurs Dr.Web sur tous les OS supportés. La configuration de l'accès au Serveur Dr.Web pour tous les utilisateurs par les attributs correspondants d'Active Directory se fait via le Centre de gestion. L'accès au contrôleur du domaine et au composant logiciel enfichable Active Directory n'est requis — une configuration supplémentaire du côté d'Active Directory n'est pas effectuée.
- Microsoft Active Directory. Disponible uniquement pour les Serveurs Dr.Web sous Windows inclus dans le domaine cible. La configuration des utilisateurs et des groupes d'utilisateurs ayant accès au Serveur Dr.Web se fait directement dans le composant logiciel enfichable Active Directory. La configuration initiale avec les utilitaires supplémentaires est requise. Les packages `drweb-<version_du_package>-<assemblage>-esuite-modify-ad-schema-<version_de_l'OS>.exe` et `drweb-<version_du_package>-<assemblage>-esuite-aduac-<version de l'OS>.msi` sont disponibles dans le référentiel du Serveur Dr.Web dans les **Produits d'entreprise Dr.Web**.

La sélection de la méthode dépend du système d'exploitation du Serveur Dr.Web et du moyen de configuration des utilisateurs autorisés.

Pour en savoir plus, voir le **Manuel d'administrateur** [Authentification des administrateurs](#).

4. Installation à distance des Agents Dr.Web sur le poste dans le domaine Active Directory

Il est possible d'installer à distance l'Agent Dr.Web sur le poste dans le domaine Active Directory. Pour ce faire :

- a) Effectuer une installation administrative sur la ressource cible partagée avec l'installateur spécial de l'Agent pour Dr.Web Active Directory. Le package `drweb-<version_du_package>-<assemblage>-esuite-agent-activedirectory.msi` est disponible dans le référentiel du Serveur Dr.Web dans le **Produits d'entreprise Dr.Web**.
- b) Configurer les politiques correspondantes d'Active Directory pour l'installation automatique du package de poste dans le domaine.

Pour en savoir plus, voir [Installation de l'Agent Dr.Web avec le service Active Directory](#).

5. Recherche des postes du domaine Active Directory

Il existe une possibilité de chercher les postes du domaine Active Directory via le Scanner du réseau. Dans ce cas, il est possible de déterminer la présence de l'Agent Dr.Web sur les postes trouvés et, s'il n'y est pas, l'installer à distance via le Centre de gestion.

Cette approche de l'installation distante des Agent Dr.Web peut être utilisée en même temps que l'installation automatique des packages avec les politiques Active Directory décrite dans le p.4.



Pour en savoir plus, voir le **Manuel d'administrateur** [Scanner réseau](#).

6. Recherche des utilisateurs du domaine Active Directory

Il existe une possibilité de chercher les utilisateur du domaine Active Directory pour la création des profils utilisateur et une configuration plus précise de Office Control et du Contrôle des applications.

Pour en savoir plus, voir le **Manuel de gestion des postes sous Windows**.



Chapitre 5 : Installation des composants Dr.Web Enterprise Security Suite

Avant d'installer les composants Dr.Web Enterprise Security Suite, veuillez consulter la section [Création d'un réseau antivirus](#).

5.1. Installation du Serveur Dr.Web

L'installation du Serveur Dr.Web est la première étape du déploiement du réseau antivirus. Aucun autre composant du réseau antivirus ne peut être installé avant que l'installation du serveur ne soit réussie.

La procédure d'installation du Serveur Dr.Web varie en fonction de la version (pour OS Windows ou pour les OS de la famille UNIX) à installer.



Tous les paramètres configurés lors de l'installation peuvent être modifiés ultérieurement par l'administrateur du réseau antivirus pendant le fonctionnement du Serveur Dr.Web.

Si le logiciel du Serveur Dr.Web est déjà installé, consultez les paragraphes [Mise à jour du Serveur Dr.Web sous Windows](#) ou [Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX](#).



Dans le cas où la suppression du Serveur Dr.Web a précédé l'installation du logiciel du Serveur Dr.Web, le contenu du référentiel sera supprimé et une nouvelle version du référentiel sera installée. Si pour une raison quelconque le référentiel de la version précédente a été conservé, il sera nécessaire de supprimer manuellement tout son contenu avant l'installation d'une nouvelle version du Serveur Dr.Web. Après l'installation du Serveur Dr.Web, il faut effectuer une mise à jour complète du référentiel.

Le nom du répertoire dans lequel le Serveur Dr.Web est installé doit être spécifié dans la langue indiquée dans les paramètres de langue pour les programmes non unicode du système Windows. Sinon le Serveur Dr.Web ne sera pas installé.

Exception : le cas où l'anglais est utilisé pour le nom du répertoire d'installation.

Le Centre de gestion de la Sécurité s'installe automatiquement avec le Serveur Dr.Web et sert à gérer le réseau antivirus et la configuration du Serveur Dr.Web.

Par défaut, sous Windows, le Serveur Dr.Web démarre de manière automatique après l'installation. Sous les OS de la famille UNIX le démarrage est effectué manuellement.



5.1.1. Installation du Serveur Dr.Web sous Windows

L'installation du Serveur Dr.Web sous Windows est décrite ci-dessous.

Avant l'installation du Serveur Dr.Web, il est recommandé de prendre en compte les informations ci-dessous :



Le fichier de la distribution et les autres fichiers requis lors de l'installation doivent se trouver sur les disques locaux du poste sur lequel le logiciel du Serveur Dr.Web sera installé. Les droits d'accès doivent être paramétrés de sorte que ces fichiers soient accessibles à l'utilisateur **LOCALSYSTEM**.

Les droits d'administrateur sur le poste sont requis pour installer le Serveur Dr.Web.



Après l'installation du Serveur Dr.Web, une mise à jour de tous les composants de Dr.Web Enterprise Security Suite est nécessaire (voir **Manuel Administrateur**, p. [Mise à jour manuelle du référentiel du Serveur Dr.Web](#)).

La [Fig. 5-1](#) présente un organigramme de la procédure d'installation du Serveur Dr.Web avec l'installateur. La description détaillée [ci-dessous](#) correspond aux étapes de la procédure.

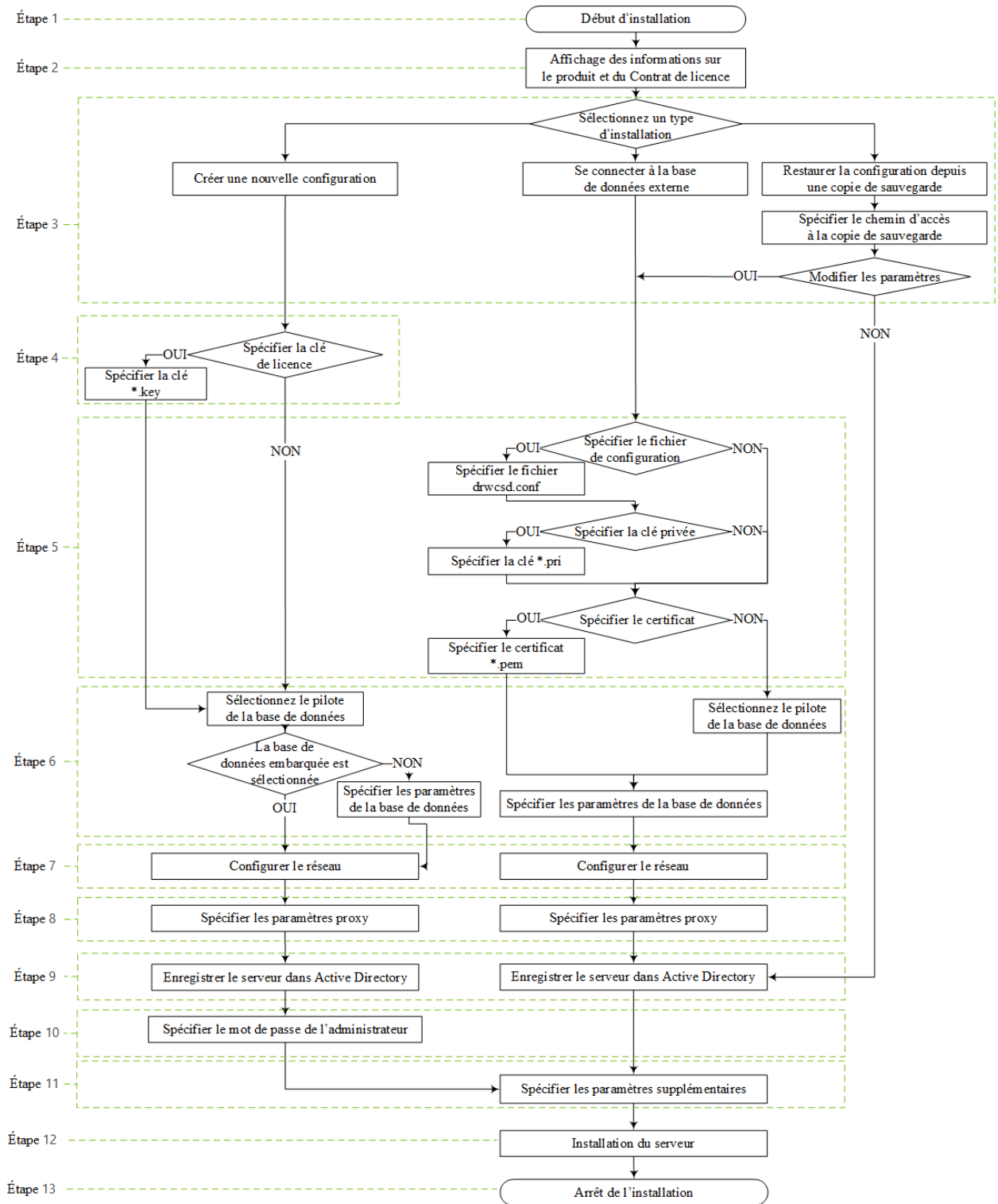


Figure 5-1. Schéma de la procédure d'installation du Serveur Dr.Web (Cliquez sur un élément de l'organigramme pour consulter la description)

Pour installer le Serveur Dr.Web sur un ordinateur tournant sous Windows

1. Lancez le fichier de distribution. La disponibilité d'une version plus récente de la distribution est vérifiée sur le SGM lors de l'installation.



Par défaut, la langue du système d'exploitation est sélectionnée comme la langue de l'installateur. Si nécessaire, vous pouvez modifier la langue d'installation à toutes les étapes en sélectionnant l'élément correspondant qui se trouve dans l'angle droit supérieur de la fenêtre de l'installateur.

2. Une fenêtre va s'ouvrir contenant les informations sur le produit installé et le lien sur le texte du Contrat de licence. Après avoir pris connaissance des termes du contrat de licence, cliquez sur **Suivant** pour continuer l'installation.
3. Dans la fenêtre suivant, sélectionnez le type d'installation du Serveur Dr.Web :
 - **Créer une nouvelle configuration** : ce type d'installation comprend la création d'une nouvelle configuration du Serveur avec les paramètres par défaut. L'utilisation des paramètres des installations précédentes du Serveur n'est pas prévue. Dans ce type d'installation, l'initialisation de la nouvelle base de données se fait indépendamment du type de la base de données sélectionné lors de la configuration. Cliquez sur **Suivant**. Allez à l'étape 4.
 - **Se connecter à la base de données externe** : ce type d'installation comprend la connexion à la base de données externe existante du Serveur. Dans ce type d'installation la base de données externe existante de l'installation précédente du Serveur est mise à jour. Cliquez sur **Suivant**. Allez à l'étape 5.



En cas d'utilisation d'une BD externe, il faut d'abord créer la BD et paramétrer ensuite le pilote correspondant (voir le document **Annexes**, [Annexe A. Description des paramètres du SGBD. Paramètres de pilotes du SGBD](#)).

- **Restaurer la configuration de la copie de sauvegarde** : tous les paramètres seront restaurés de la copie de sauvegarde de l'installation précédente du Serveur. Spécifiez le chemin d'accès à la copie de sauvegarde. Dans ce type d'installation, l'importation se fait avec la mise à jour du dump de la base de données de la copie de sauvegarde.
 - Si nécessaire, vous pouvez modifier les paramètres tirés de la copie de sauvegarde manuellement. Pour ce faire, cliquez sur le bouton **Modifier les paramètres** - les paramètres des étapes 5-8 seront disponibles.
 - S'il n'y a pas la nécessité de modifier les paramètres manuellement, cliquez sur **Suivant**. L'utilisation de la configuration tirée de la copie de sauvegarde va se faire automatiquement. La clé de chiffrement privée et le certificat seront tirés de la copie de sauvegarde. La présence du fichier de configuration est obligatoire pour la continuation de l'installation. Si l'Assistant ne pourra pas restaurer certains paramètres de la copie de sauvegarde, une fenêtre s'affichera dans laquelle vous pourrez spécifier les paramètres manuellement. Accédez à l'étape 9.
4. Si à l'étape 3 vous avez choisi l'option **Créer une nouvelle configuration** spécifiez les paramètres d'octroi de licence dans la fenêtre **Licence** :
 - Sélectionnez l'option **Configurer l'octroi de licence plus tard** pour continuer l'installation du Serveur sans clé de licence.
Notez que pour l'organisation du système proxy de postes une licence est requise. Les clés



de licence doivent être ajoutées après l'installation du Serveur Dr.Web, via le [Gestionnaire de licences](#) ou bien, le nombre nécessaire de licences doit être transmis par la liaison entre les serveurs depuis le Serveur voisin.

- La case **Spécifier la clé de licence** permet de spécifier le fichier clé de licence de l'Agent Dr.Web lors de l'installation du Serveur.

Pour tester le produit, vous pouvez utiliser des fichiers clés de démonstration. Cliquez sur le bouton **Demander une clé de démonstration** pour visiter le site web de Doctor Web et obtenir les fichiers clés de démo (voir [Fichiers clés de démonstration](#)).

5. Si à l'étape 3 vous avez sélectionné l'option **Se connecter à la base de données externe** ou que vous avez sélectionné l'élément **Modifier les paramètres** lors de la restauration de la configuration de la copie de sauvegarde, vous pouvez spécifier les paramètres suivants dans la fenêtre **Configuration du Serveur Dr.Web** :

- **Fichier de configuration du Serveur Dr.Web** : chemin d'accès au fichier de configuration avec les paramètres du Serveur Dr.Web de l'installation précédente (`drwcsd.conf`).
- **Clé de chiffrement privée du Serveur Dr.Web** : chemin d'accès au fichier contenant la clé de chiffrement privée du Serveur de l'installation précédente. Dans ce cas, un fichier contenant la clé publique sera créée (le contenu de la clé publique correspondra au contenu de la clé publique précédente) ainsi que le certificat, s'il n'est pas spécifié dans le champ ci-dessous (à chaque génération de la même clé privée, un nouveau certificat est créé).
- Si vous utilisez la clé de chiffrement privée existante, spécifiez le fichier de certificat qui a été utilisé auparavant dans le champ **Utiliser le certificat existant du Serveur Dr.Web**. Ceci permettra aux Agents Dr.Web déjà installés de se connecter au nouveau Serveur Dr.Web car les clients connectés au Serveur Dr.Web sont liés à un certificat particulier (à chaque génération de la même clé privée, un nouveau certificat est créé). Sinon, après l'installation, il sera nécessaire de copier le nouveau certificat sur tous les postes sur lesquels les Agents Dr.Web ont été installés précédemment.



Le certificat doit correspondre à la clé de chiffrement privée.

Si les chemins d'accès aux fichiers ne sont pas spécifiés, les nouvelles clés de chiffrement, le certificat et le fichier de configuration avec les paramètres par défaut seront créés.

6. La fenêtre **Pilote de la base de données** permet de configurer les paramètres de la base de données utilisée. Ces paramètres dépendent du type d'installation :
- Si à l'étape 3 vous avez choisi l'option **Créer une nouvelle configuration**, sélectionnez le type de pilote qu'il faut utiliser :
 - L'option **SQLite (base de données embarquée)** active l'utilisation des outils intégrés du Serveur Dr.Web. La définition de paramètres supplémentaires n'est pas requise.
 - Les autres options correspondent à l'utilisation d'une BD externe. Dans ce cas, il faut d'abord indiquer les paramètres correspondants pour la configuration d'accès à la BD. La configuration des paramètres du SGBD est décrite dans les Annexes (voir le



document **Annexes**, [Annexe A. Paramètres d'utilisation du SGBD. Paramètres des pilotes du SGBD](#)).

- Si à l'étape 3 vous avez sélectionné l'option **Se connecter à la base de données externe** ou que vous avez coché la case **Modifier les paramètres** pour l'option **Se connecter à la base de données externe** :
 - Si à l'étape 5 vous avez spécifié le chemin d'accès au fichier de configuration du Serveur, les données du fichier de configuration seront tirées automatiquement. Si nécessaire, modifiez-les.
 - Si à l'étape 5 vous n'avez pas spécifié le chemin d'accès au fichier de configuration du Serveur, sélectionnez un pilote de la base de données externe et spécifiez les paramètres de la base de données à laquelle se connectera le Serveur.
- 7. Si à l'étape 3 vous avez sélectionné l'option **Créer une nouvelle configuration** ou **Se connecter à la base de données externe** que vous avez coché la case **Modifier les paramètres** pour l'option **Se connecter à la base de données externe**, la fenêtre **Configuration du réseau** va s'afficher. Dans cette fenêtre vous pouvez configurer le protocole réseau pour le fonctionnement du Serveur (il est autorisé de spécifier un seul protocole réseau, les protocoles supplémentaires vous pouvez spécifier ultérieurement).
 - Dans les champs **Interface** et **Port**, spécifiez les valeurs correspondantes pour l'accès au Serveur.



Le port 2193 est utilisé par défaut.

Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).

- Cochez la case **Activer le service de détection du Serveur Dr.Web** si vous souhaitez que le Serveur réponde aux requêtes de recherche multicast ou broadcast de la part des autres Serveurs via l'adresse IP et le nom du service spécifiés dans les champs correspondants ci-dessous.
8. Si à l'étape 3 vous avez sélectionné l'option **Créer une nouvelle configuration** ou **Se connecter à la base de données externe** ou que vous avez coché la case **Modifier les paramètres** pour l'option **Se connecter à la base de données externe**, la fenêtre **Serveur proxy** va s'afficher. Dans la fenêtre vous pouvez configurer les paramètres d'utilisation du serveur proxy lors de la connexion au Serveur Dr.Web.

Pour se connecter au Serveur via le serveur proxy cochez la case **Utiliser le serveur proxy**.



La case **Utiliser le Serveur proxy** sera disponible uniquement si le dossier d'installation du Serveur ne contient pas de fichiers de configuration de l'installation précédente.

Définissez les paramètres suivants pour configurer la connexion au serveur proxy :

- **Adresse du serveur proxy** : adresse IP ou nom DNS du serveur proxy (champ obligatoire),
- **Nom d'utilisateur, Mot de passe** : nom d'utilisateur et mot de passe d'accès au serveur proxy, si le serveur proxy supporte la connexion authentifiée.



- Dans la liste déroulante **Méthode d'authentification**, sélectionnez la méthode d'authentification sur le serveur proxy s'il supporte les connexions authentifiées.
9. Si l'ordinateur sur lequel l'installation du Serveur est effectuée, fait partie du domaine Active Directory, vous serez invité à enregistrer le Serveur Dr.Web dans le domaine Active Directory dans la fenêtre suivante. Lors de l'enregistrement dans le domaine Active Directory sur le serveur DNS, l'enregistrement SRV correspondant au Serveur Dr.Web sera créé. Après les clients pourront accéder au Serveur Dr.Web via cet enregistrement SRV.

Pour enregistrer, configurez les paramètres suivants :

- Cochez la case **Enregistrer le Serveur Dr.Web dans Active Directory**.
 - Dans le champ **Domaine** indiquez le nom du domaine Active Directory, dans lequel le Serveur sera enregistré. Si le domaine n'est pas spécifié, ce sera le domaine dans lequel est enregistré l'ordinateur que lequel l'installation est effectuée qui sera utilisé.
 - Dans les champs **Nom d'utilisateur** et **Mot de passe** entrez les identifiants de l'administrateur du domaine Active Directory.
 - Les adresses des **Serveurs DNS** sont extraites automatiquement et leur nombre dépend des serveurs DNS spécifiés.
10. Si à l'étape 3 vous avez sélectionné l'option **Créer une nouvelle configuration**, la fenêtre **Mot de passe de l'administrateur** va s'ouvrir. Spécifiez le mot de passe de l'administrateur du réseau antivirus, créé par défaut avec l'identifiant **admin** et un accès à toutes les options de gestion du réseau antivirus.

Dans les autres types d'installation, le mot de passe de l'administrateur principal sera tiré de la base de données de l'installation précédente du Serveur.

11. Dans la fenêtre suivant l'Assistant vous informera sur la disponibilité de l'installation du Serveur Dr.Web. Si nécessaire, vous pouvez configurer les paramètres d'installation avancés. Pour ce faire cliquez sur l'élément **Paramètres avancés** en bas de la fenêtre et définissez les paramètres suivants :

- Dans l'onglet **Général** :
 - Dans liste déroulante **Langue d'interface du Centre de gestion de la sécurité Dr.Web**, sélectionnez la langue d'interface par défaut pour le Centre de gestion de la sécurité Dr.Web.
 - Dans la liste déroulante **Langue d'interface de l'Agent Dr.Web**, sélectionnez la langue d'interface par défaut pour l'Agent Dr.Web et pour les composants du package antivirus installés sur les postes.
 - Cochez la case **Partager le dossier d'installation de l'Agent Dr.Web** pour modifier le mode d'utilisation et le nom du dossier d'installation partagé de l'Agent Dr.Web (le nom masqué des ressources partagées est défini par défaut).
 - Cochez la case **Démarrer le Serveur Dr.Web** après l'installation pour démarrer automatiquement le Serveur Dr.Web après l'installation.
 - Cochez la case **Mettre à jour le référentiel après la fin de l'installation** pour mettre à jour automatiquement le référentiel du Serveur Dr.Web juste après la fin de l'installation.



- Pour restreindre l'accès local au Serveur, cochez la case **Restreindre l'accès au Serveur Dr.Web**. Ainsi l'accès sera interdit aux installateurs des Agents Dr.Web, aux Agents Dr.Web et aux autres Serveurs (en cas de réseau antivirus existant créé à l'aide de Dr.Web Enterprise Security Suite). Vous pouvez modifier ces paramètres ultérieurement depuis le menu du Centre de gestion **Administration**, élément **Configuration du Serveur Dr.Web**, onglet **Modules**.
- Cochez la case **Envoyer des statistiques à Doctor Web** pour autoriser l'envoi des statistiques sur les événements viraux à Doctor Web.
- Dans l'onglet **Chemin** :
 - Dans le champ **Répertoire d'installation du Serveur Dr.Web** est spécifié le répertoire dans lequel l'installation du Serveur Dr.Web est effectuée. Pour modifier le répertoire spécifié par défaut cliquez sur **Parcourir** et sélectionnez le répertoire nécessaire.
 - Dans le champ **Répertoire de sauvegarde du Serveur Dr.Web** est spécifié le répertoire dans lequel la sauvegarde des données critiques du Serveur est effectuée d'après les tâches du planificateur du Serveur Dr.Web. Pour modifier le répertoire spécifié par défaut cliquez sur **Parcourir** et sélectionnez le répertoire nécessaire.
- Dans l'onglet **Journal**, vous pouvez configurer la journalisation du fonctionnement du Serveur Dr.Web.

Après avoir configuré les composants supplémentaires cliquez sur **OK** pour appliquer les modifications ou sur **Annuler** si vous n'avez apporté aucune modification ou pour annuler les modifications apportées.

12. Cliquez sur le bouton **Installer** afin de lancer la procédure d'installation. Les actions suivantes du logiciel ne nécessitent aucune intervention de l'utilisateur.

13. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

La gestion du Serveur Dr.Web est effectuée normalement à l'aide du Centre de gestion qui sert d'interface intégrée pour le Serveur Dr.Web.

Les éléments qui permettent de faciliter et de paramétrer la gestion du Serveur Dr.Web sont placés lors de l'installation du Serveur Dr.Web dans le répertoire **Dr.Web Server** du menu principal de Windows **Programmes** :

- Le répertoire **Gestion du serveur** contient les commandes de démarrage, de redémarrage et d'arrêt du Serveur Dr.Web, ainsi que les commandes déterminant le mode de journalisation et d'autres commandes du Serveur Dr.Web décrites dans le document **Annexes**, [G3. Serveur Dr.Web](#).
- L'élément **Interface Web** permet d'ouvrir le Centre de gestion et de se connecter au Serveur Dr.Web installé sur ce poste (à l'adresse <https://localhost:9081>).
- L'élément **Documentation** sert à afficher le Manuel Administrateur au format HTML.

La structure du dossier d'installation du Serveur Dr.Web est décrite dans le **Manuel Administrateur**, à la rubrique [Serveur Dr.Web](#).



5.1.2. Installation du Serveur Dr.Web pour les OS de la famille UNIX



Toutes les actions relatives à l'installation doivent être effectuées depuis la console sous le nom de super-utilisateur (**root**).

Pour installer le Serveur Dr.Web pour les OS de la famille UNIX

1. Pour démarrer l'installation du package du Serveur Dr.Web, exécutez la commande suivante :

```
./<fichier_de_distribution>.tar.gz.run
```



Pour lancer le package d'installation, vous pouvez utiliser les clés de la ligne de commande. Vous trouverez les paramètres de la commande de démarrage dans les **Annexes**, [G6. Installateur du Serveur Dr.Web pour les OS de la famille UNIX](#).

Le nom par défaut de l'administrateur du réseau antivirus est **admin**.

2. Les fenêtres suivantes contiennent le Contrat de licence. Pour procéder à l'installation, vous devez l'accepter.
3. Pour utiliser la configuration de la précédente installation stockée dans une copie de sauvegarde, saisissez le chemin d'accès au dossier contenant la copie de sauvegarde (ou appuyez sur la touche ENTREE pour utiliser le répertoire par défaut — `/var/tmp/drwcs`). Pour installer le Serveur Dr.Web sans utiliser la configuration précédente, saisissez 0.
4. Si une distribution supplémentaire (extra) est trouvée dans le système, la notification sur la suppression de la distribution supplémentaire sera affichée avant le début de l'installation du package du Serveur Dr.Web. Il n'est pas possible de continuer l'installation sans supprimer la distribution supplémentaire.
5. Les composants seront ensuite installés sur votre ordinateur. Au cours de l'installation, vous pouvez être sollicités pour confirmer certaines actions en tant qu'administrateur.
6. Lors de l'installation un mot de passe aléatoire est généré pour l'administrateur principal. Après la fin de l'installation, ce mot de passe s'affiche via la console dans les résultats de l'installation du Serveur Dr.Web.



Au cours de l'installation du logiciel sous l'OS **FreeBSD** un script `rc- /usr/local/etc/rc.d/drwcsd` sera créé.

Utilisez les commandes :

- `/usr/local/etc/rc.d/drwcsd stop` : pour arrêter manuellement le Serveur Dr.Web ;
- `/usr/local/etc/rc.d/drwcsd start` : pour le lancement manuel du Serveur Dr.Web.



En cas de première installation du Serveur Dr.Web, la clé de licence n'est pas spécifiée. Les clés de licence doivent être ajoutées après l'installation du Serveur Dr.Web, via le [Gestionnaire de licences](#).

Configuration d'Astra Linux en version 1.6 pour l'installation du Serveur Dr.Web en mode ELF

En cas d'installation du Serveur Dr.Web dans l'environnement Astra Linux en version 1.6 fonctionnant en mode ELF (environnement logiciel fermé), vous pouvez échouer à lancer l'installateur si la clé de chiffrement publique du Serveur Dr.Web n'est pas présente dans la liste des clés de confiance. Dans ce cas il faut reconfigurer le mode ELF et redémarrer l'installateur.

Pour reconfigurer le mode ELF

1. Installez le paquet `astra-digsig-oldkeys` depuis le disque de l'OS s'il n'est pas encore installé.
2. Placez la clé publique de chiffrement du Serveur Dr.Web dans le répertoire `/etc/digsig/keys/legacy/keys` (s'il n'y a pas le répertoire, il faut le créer).
3. Exécutez la commande suivante :

```
# update-initramfs -k all -u
```

4. Redémarrez le système.

Configuration d'Astra Linux Special Edition avec PostgreSQL en cas d'utilisation du contrôle d'accès obligatoire

Pour configurer PostgreSQL pour le fonctionnement avec le contrôle d'accès obligatoire `/etc/postgresql/<version_de_la_BD>/main/postgresql.conf`, spécifiez la valeur `false` pour le paramètre `ac_ignore_socket_maclabel`. Une fois la valeur spécifié, le serveur du SGBD vérifiera l'étiquette de sécurité de chaque connexion entrante et ne transmettra que les informations possédant une étiquette égale ou inférieure à celle de connexion entrante.

```
ac_ignore_socket_maclabel = false
```

5.2. Installation de l'Agent Dr.Web



Les droits d'administrateur sur le poste sont requis pour installer l'Agent Dr.Web.



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.

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.

L'Agent Dr.Web peut être installé sur un poste de travail par un des moyens suivants :

1. [En mode local.](#)

L'installation en mode local est effectuée directement sur l'ordinateur ou sur l'appareil mobile de l'utilisateur. Elle peut être réalisée soit par l'administrateur, soit par l'utilisateur.

2. [En mode distant.](#)

L'installation à distance s'effectue depuis le Centre de gestion via LAN. L'installation est effectuée par l'administrateur du réseau antivirus sans aucune intervention de l'utilisateur.

Installation de l'Agent Dr.Web par-dessus le produit antivirus autonome Dr.Web pour les postes tournant sous Windows

Si le produit autonome Dr.Web en version 7.x-12.x est déjà installé sur le poste tournant sous Windows, l'installation de l'Agent Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0 s'effectue d'après le schéma suivant :

- En cas de lancement de l'installateur ou du package d'installation de l'Agent Dr.Web en mode GUI sur le poste contenant le produit autonome installé en version 7.x-12.x l'installateur du produit installé sera lancé. Puis, l'utilisateur sera invité à entrer le code de confirmation d'actions et à supprimer le produit. Après le redémarrage de l'OS, la version GUI de l'installateur qui a été lancé initialement pour l'installation de l'Agent Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0, sera lancée.
- Si l'installateur de l'Agent Dr.Web est lancé en tâche de fond sur le poste contenant le produit autonome en version 7.x-12.x, cela ne va pas aboutir à l'exécution des actions quelconques. En cas de [l'installation à distance](#), l'installateur va informer le Centre de gestion de la présence des produits autonomes en versions précédentes. Dans ce cas, il est nécessaire de supprimer manuellement le produit autonome et d'installer l'Agent Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0 par un des moyens possibles.
- En cas d'installation locale ou distante de l'Agent Dr.Web sur le poste contenant le produit autonome en version 13.0, le produit installé va basculer du mode autonome en mode de protection centralisée. Après la connexion et l'authentification sur le Serveur Dr.Web, il est possible d'obtenir des mises à jour, de nouvelles configurations et la liste de composants à installer. Certains composants peuvent exiger un redémarrage.



Lors de l'installation des Agents Dr.Web sur les serveurs de LAN et sur les ordinateurs du cluster, il faut prendre en compte les informations suivantes :

- En cas d'installation sur les ordinateurs servant des serveurs terminaux (sous Windows les services **Terminal Services** sont installés), afin d'assurer le fonctionnement des Agents Dr.Web lors des sessions terminales des utilisateurs, il est recommandé d'effectuer l'installation des Agents Dr.Web de manière locale avec l'assistant d'installation et de suppression des programmes depuis le **Panneau de configuration** Windows. L'installation distante dans ce cas peut provoquer des erreurs de fonctionnement du protocole Remote Desktop.
- Il n'est pas recommandé d'installer les composants SpIDer Gate, Office Control, SpIDer Mail et le Pare-feu Dr.Web sur les serveurs exécutant des fonctions réseau importantes (contrôleurs de domaine, serveurs de distribution des licences etc.) afin d'éviter d'éventuels conflits entre les services réseau et les composants intérieurs de l'antivirus Dr.Web.
- L'installation de l'Agent Dr.Web sur le cluster doit être réalisée séparément pour chaque nœud du cluster.
- Les principes de fonctionnement de l'Agent Dr.Web et des composants du package antivirus sur un hôte du cluster sont équivalents aux principes relatifs à un serveur LAN, c'est pourquoi il n'est pas recommandé d'installer sur les hôtes du cluster les composants SpIDer Gate, SpIDer Mail et le Pare-feu Dr.Web.
- Si l'accès à la ressource quorum du cluster est strictement limité, il est recommandé de l'exclure de l'analyse par le moniteur SpIDer Guard et de se contenter de l'analyse régulière de cette ressource par le Scanner, lancé selon la planification ou manuellement.

5.2.1. Fichiers d'installation

Packages d'installation

Package d'installation personnel

Lors de la création d'un nouveau compte pour un poste, un package d'installation personnel de l'Agent Dr.Web est généré dans le Centre de gestion. Le package d'installation personnel inclut l'installateur de l'Agent Dr.Web et le jeu de paramètres de connexion et d'authentification du poste sur le Serveur Dr.Web.

Les packages d'installation personnels sont disponibles pour les postes protégés tournant sous tous les systèmes d'exploitation supportés par Dr.Web Enterprise Security Suite. Les packages d'installation personnels sont créés dans le Centre de gestion à la base de l'[installateur](#) de l'Agent Dr.Web. Les paramètres de connexion et d'authentification du poste sur le Serveur Dr.Web sont inclus directement dans le package d'installation personnel.



Pour obtenir les packages d'installation personnels sous les systèmes d'exploitation autres que Windows, après l'installation du Serveur Dr.Web, il faut télécharger dans le référentiel les produits d'entreprise Dr.Web correspondants se trouvant sur les serveurs du SGM.

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

Le lien de téléchargement du package d'installation personnel de l'Agent Dr.Web sur un poste particulier est disponible :

1. Immédiatement après la création d'un nouveau poste (voir étape **11** dans la rubrique [Création d'un nouveau compte](#)).
2. A n'importe quel moment après la création du poste :
 - dans la rubrique propriétés du poste,
 - dans la rubrique **Objets sélectionnés** lors de la sélection du poste depuis l'arborescence.

Package d'installation de groupe

Le package d'installation de groupe de l'Agent Dr.Web est généré dans le Centre de gestion pour l'installation sur le poste d'un groupe utilisateur particulier. Dans ce cas, l'Agent Dr.Web est installé sur tous les postes tournant sous le même OS du même package d'installation de groupe.

Le package d'installation de groupe inclut l'installateur de l'Agent Dr.Web, les paramètres de connexion au Serveur Dr.Web, ainsi que l'identificateur et le mot de passe du groupe utilisateur dans lequel le poste sera inclus après l'installation de l'Agent Dr.Web. Pourtant les paramètres d'authentification du poste sur le Serveur Dr.Web et les composants antivirus ne sont pas inclus dans le package d'installation de groupe.

Le lien de téléchargement du package d'installation de groupe est disponible dans la rubrique de paramètres du groupe utilisateur.

Installateurs

La différence entre l'installateur de l'Agent Dr.Web et le package d'installation est que le premier ne contient pas les paramètres de connexion et d'authentification de poste sur le Serveur Dr.Web.

Les installateurs suivants de l'Agent Dr.Web sont fournis :

- Pour les postes tournant sous Windows, deux types d'installateurs sont disponibles :
 - *L'installateur réseau* `drwinst.exe` n'installe que l'Agent Dr.Web. Après la connexion au Serveur Dr.Web, l'Agent Dr.Web télécharge et installe les composants correspondants de ce package antivirus. À l'aide de l'installateur réseau il est possible d'effectuer l'installation de l'Agent en mode local ainsi qu'à distance.



L'installateur réseau de l'Agent Dr.Web `drwinst.exe` se trouve dans le répertoire `webmin/install/windows` (par défaut, c'est une ressource partagée cachée) du répertoire d'installation du Serveur Dr.Web. L'accessibilité de cette ressource via le réseau peut être configurée à l'[étape 12](#) pendant l'installation du Serveur Dr.Web. Vous pouvez modifier cette ressource ultérieurement.

- L'*installateur complet* `drweb-<version_de_l'agent>-<assemblage>-esuite-agent-full-windows.exe` effectue l'installation de l'Agent Dr.Web et du package antivirus en même temps.
- L'installateur pour l'installation de l'Agent Dr.Web, équivalent à l'installateur de la version autonome, est disponible pour les postes tournant sous les OS Android, Linux, macOS.

L'installateur de l'Agent Dr.Web et la clé publique de chiffrement sont disponibles depuis la [page d'installation](#) du Centre de gestion de la sécurité Dr.Web.



Pour obtenir les installateurs sous les systèmes d'exploitation autres que Windows et pour installer la distribution complète de l'installateur sous Windows, après l'installation du Serveur Dr.Web, il faut télécharger dans le référentiel les produits d'entreprise Dr.Web correspondants depuis les serveurs du SGM.

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](#).

Page d'installation

Juste après l'installation du Serveur Dr.Web, sur la page d'installation du Centre de gestion de la sécurité Dr.Web, vous pourrez télécharger :

1. Installateur de l'Agent Dr.Web pour Windows.
2. Certificat du Serveur Dr.Web `drwcsd-certificate.pem`.

Après l'exécution d'une [petite configuration](#) sur la page, un ensemble d'installateurs supplémentaires sera disponible. Les installateurs pour tous les postes protégés sous tous les OS supportés par Dr.Web Enterprise Security Suite, se trouvent dans des répertoires avec les noms correspondant au nom de l'OS.

La page d'installation est accessible sur n'importe quel ordinateur ayant un accès réseau au Serveur Dr.Web, à l'adresse suivante :

`http://<Adresse_du_Serveur_Dr.Web>:<numéro_du_port>/install/`

comme `<Adresse_du_Serveur_Dr.Web>` spécifiez l'adresse IP ou le nom de domaine de l'ordinateur sur lequel le Serveur Dr.Web est installé. Comme `<numéro_du_port>`, spécifiez le port 9080 (ou 9081 pour https).



Pour configurer le contenu de produits sur la page d'installation

1. Sélectionnez l'élément **Administration** du menu principal. Ensuite, dans le menu de gestion, sélectionnez la section **Configuration générale du référentiel**.
2. Accédez à l'onglet **Packages d'installation Dr.Web** → **Produits d'entreprise Dr.Web**.
3. Cliquez sur la flèche à gauche du produit nécessaire et spécifiez le système d'exploitation et le nombre de bits. Après avoir coché les cases contre tous les produits nécessaires, cliquez sur **Enregistrer**.
4. Mettez à jour le référentiel via la section **Statut du référentiel** dans le menu de gestion.
5. Après le téléchargement depuis le SGM et la mise à jour du référentiel, les installateurs des produits sélectionnés seront disponibles sur la page d'installation.

5.2.2. Installation de l'Agent Dr.Web en mode local

L'installation de l'Agent Dr.Web en mode local est effectuée directement sur l'ordinateur ou sur l'appareil mobile de l'utilisateur. Elle peut être réalisée soit par l'administrateur, soit par l'utilisateur.



Avant la première installation des Agents Dr.Web, il est nécessaire de mettre à jour le référentiel du Serveur Dr.Web (voir **Manuel Administrateur**, p. [Mise à jour manuelle du référentiel du Serveur Dr.Web](#), p. **Vérification des mises à jour**).

Postes tournant sous Android, Linux, macOS

Pour installer l'Agent Dr.Web sur les postes tournant sous l'OS Android, OS Linux, macOS, les moyens suivants sont disponibles :

- [Package d'installation personnel](#) créé dans le Centre de gestion.
- [Package d'installation de groupe](#) créé dans le Centre de gestion.
- [Installateur](#) de l'Agent Dr.Web.

Lors de la sélection du type de package d'installation, prenez en compte les particularités suivantes :

- a) L'installateur de l'Agent Dr.Web est fourni lors de la création du package d'installation personnel, ainsi que les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web.
- b) En cas de l'installation de l'Agent Dr.Web à l'aide de l'installateur, les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web ne sont pas fournis.



Postes tournant sous l'OS Windows

Pour installer l'Agent Dr.Web en mode local sur les postes tournant sous l'OS Windows, les moyens suivants sont disponibles :

- **Package d'installation personnel** créé dans le Centre de gestion `drweb_es_<OS>_<poste>.exe`.
- **Package d'installation de groupe** créé dans le Centre de gestion `drweb_es_<OS>_<groupe>.exe`.
- **L'installateur complet** de l'Agent Dr.Web `drweb-<version_de_l'agent>-<assemblage>-esuite-agent-full-windows.exe`.
- **Installateur réseau** de l'Agent Dr.Web `drwinst.exe`.

Lors de la sélection du type de package d'installation, prenez en compte les particularités suivantes :

- a) Lors de l'installation depuis le package d'installation personnel, les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification sur le Serveur Dr.Web sont inclus dans le package d'installation personnel. L'installation depuis le package d'installation personnel est effectuée à la base de l'installateur réseau depuis lequel l'Agent Dr.Web est installé. Après la connexion au Serveur Dr.Web, l'Agent Dr.Web télécharge et installe les composants du package antivirus.
- b) Lors de l'installation depuis le package d'installation de groupe, les paramètres de connexion au Serveur Dr.Web, ainsi que l'identificateur et le mot de passe du groupe utilisateur dans lequel le poste sera inclus après l'installation de l'Agent Dr.Web, sont inclus dans le package d'installation. Pourtant les paramètres d'authentification du poste sur le Serveur Dr.Web et les composants antivirus ne sont pas inclus dans le package d'installation de groupe. Après l'installation de l'Agent Dr.Web, il établit la connexion au Serveur Dr.Web lors de laquelle l'Agent Dr.Web détermine la disponibilité de postes libres dans le groupe utilisateur, dont le package d'installation de groupe a été utilisé. Si les postes libres sont disponibles, les paramètres d'authentification du poste sur le Serveur Dr.Web sont fournis automatiquement.
- c) En cas de l'installation à l'aide de l'installateur réseau, seul l'Agent est installé. Après la connexion au Serveur Dr.Web, l'Agent Dr.Web télécharge et installe les composants correspondants du package antivirus. Dans ce cas, les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web ne sont pas fournis.
- d) En cas de l'installation à l'aide de la distribution complète, l'Agent Dr.Web et le package d'installation sont installés simultanément. Dans ce cas, les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web ne sont pas fournis.



Caractéristiques comparatives des fichiers d'installation

Fichier d'installation		Installation de l'Agent Dr.Web	Installation du package antivirus	Paramètres de connexion au Serveur Dr.Web	Paramètres d'authentification sur le Serveur Dr.Web
Package d'installation	Personnel	+	-	+	+
	de groupe	+	-	+	-
Installeur	Réseau	+	-	-	-
	Complet	+	+	-	-



Pour obtenir les installeurs et les packages d'installation sous les OS autres que Windows et pour installer la distribution complète de l'installeur sous Windows, après l'installation du Serveur Dr.Web, il faut télécharger dans le référentiel les **Produits d'entreprise Dr.Web** se trouvant sur les serveurs du SGM.

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](#).



Le lancement de fichiers d'installation de l'Agent Dr.Web de tout type est également possible depuis la ligne de commande à l'aide de clés mentionnées dans le document **Annexes**, p. [G1. Installeur réseau](#).

5.2.2.1. Installation de l'Agent Dr.Web avec le package d'installation personnel

Pour installer l'Agent Dr.Web sur les postes avec le package d'installation personnel

1. Depuis le Centre de gestion [créez un compte](#) de nouveau poste sur le Serveur Dr.Web.
2. Si l'utilisateur effectue l'installation de l'Agent Dr.Web lui-même, envoyez-lui le lien vers le package d'installation personnel de l'Agent Dr.Web pour le système d'exploitation correspondant de l'ordinateur ou de l'appareil mobile.



Pour transmettre facilement le fichier d'installation et le fichier de configuration, vous pouvez utiliser la fonction **Envoi des fichiers d'installation** (pour plus d'information, consultez le **Manuel Administrateur**, p. [Envoi des fichiers d'installation](#)). Ainsi, vous pourrez envoyer un message contenant les fichiers correspondants sur l'e-mail.

3. Effectuez l'installation de l'Agent Dr.Web sur le poste de travail.



L'installation de l'Agent Dr.Web en mode local sur le poste de travail est décrite dans le **Manuel Utilisateur** pour les OS correspondants.



Les droits d'administrateur sur le poste sont requis pour installer l'Agent Dr.Web.

Si un antivirus est déjà installé sur le poste, avant de procéder à l'installation, le package d'installation personnel va essayer de le supprimer. En cas d'échec, l'utilisateur doit désinstaller le logiciel antivirus opérant sur le poste lui-même.

4. Pour les postes sous macOS, [configurez les paramètres de connexion](#) au Serveur Dr.Web de manière locale.

En cas de l'installation de l'Agent Dr.Web à l'aide du package d'installation personnel pour les autres systèmes supportés, la configuration supplémentaire n'est pas requise. Les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web sont inclus directement dans le package d'installation personnel. Après l'installation de l'Agent Dr.Web, le poste va se connecter au Serveur Dr.Web automatiquement.

Création d'un nouveau compte de poste

Afin de créer un compte ou plusieurs comptes de nouveaux postes, utilisez le Centre de gestion de la sécurité Dr.Web.



Lors de la création d'un compte de poste, notez le nom du Serveur Dr.Web indiqué dans les sections suivantes du Centre de gestion :

1. **Administration** → **Configuration du Serveur web** → champ **Adresse du Serveur Dr.Web**. La valeur de ce paramètre est utilisée lors de la génération du lien vers le package d'installation de l'Agent Dr.Web.
Si la valeur de ce paramètre n'est pas spécifiée, le nom DNS (s'il est disponible) ou l'adresse IP de l'ordinateur sur lequel le Centre de gestion est ouvert est utilisé en tant que nom du Serveur Dr.Web pour générer le lien de téléchargement du package d'installation personnel de l'Agent Dr.Web.
2. **Administration** → **Configuration du Serveur Dr.Web** → Onglet **Réseau** → onglet **Téléchargement** → champ **Adresse du Serveur Dr.Web**. La valeur de ce paramètre est spécifiée dans les packages d'installation de l'Agent Dr.Web et définit à quel Serveur Dr.Web l'Agent Dr.Web sera connecté durant l'installation.

Si la valeur du paramètres n'est pas spécifiée, lors de la création du package d'installation de l'Agent Dr.Web, l'adresse du Serveur Dr.Web auquel est connecté le Centre de gestion est spécifiée. Dans ce cas, le Centre de gestion doit être connecté au Serveur Dr.Web utilisant l'adresse IP du domaine pour lequel vous avez créé un compte (l'adresse du Serveur Dr.Web ne doit pas être spécifiée comme un loopback — 127.0.0.1).




Pour créer un nouveau compte de poste depuis le Centre de gestion de la sécurité Dr.Web

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la barre d'outils, cliquez sur le bouton **+ Ajouter un objet de réseau** → **+ Créer un poste**. Le panneau de création du compte du poste sera affiché dans la partie droite de la fenêtre du Centre de gestion.
3. Spécifiez le nombre des comptes à créer dans le champ **Nombre**.
4. L'identificateur unique du poste sera spécifié de manière automatique dans le champ **Identificateur**. Si nécessaire, vous pouvez le modifier.
5. Dans le champ **Nom**, spécifiez le nom du poste à afficher dans l'arborescence du réseau antivirus. Par la suite, après la connexion du poste au Serveur Dr.Web, ce nom peut être automatiquement remplacé par le nom spécifié de manière locale.
6. Dans les champs **Mot de passe** et **Confirmez le mot de passe**, entrez le mot de passe nécessaire pour que le poste puisse accéder au Serveur Dr.Web. Si le mot de passe n'est pas spécifié, il sera généré automatiquement.



En cas de création de plusieurs comptes, les champs **Identificateur**, **Nom** et **Mot de passe** (**Confirmez le mot de passe**) seront remplis de manière automatique et il sera impossible de les modifier durant la création des postes.

7. Dans le champ **Description**, entrez des informations supplémentaires sur le poste. Ce paramètre est facultatif.
8. Dans la section **Groupes**, sélectionnez les groupes auxquels va appartenir le poste que vous créez.
 - Dans la liste **Appartenance à**, vous pouvez configurer la liste de groupes utilisateur auxquels va appartenir le poste.

Par défaut, le poste fait partie du groupe **Everyone**. S'il existe des groupes utilisateur, vous pouvez y inclure le poste que vous créez sans aucune restriction du nombre de groupes auxquels appartient le poste. Pour ce faire, cliquez sur **Modifier** , cochez les cases contre les groupes utilisateur nécessaires dans la liste **Appartenance** et cliquez sur **Appliquer**.




Il est impossible d'exclure le poste du groupe **Everyone** ou du groupe primaire.

Pour spécifier le groupe primaire pour le poste en cours de création, cliquez sur l'icône du groupe sélectionné dans la section **Appartenance**. Le caractère **1** s'affichera dans l'icône du groupe.


- Dans la liste **Politiques**, vous pouvez spécifier la politique dont les paramètres seront utilisés pour le poste créé.

La liste s'affiche si la case **Utiliser les politiques** est cochée dans l'onglet **Général** de la section **Administration** → **Configuration du Serveur Dr.Web**.



Par défaut, la politique n'est pas assignée. Pour assigner la politique, cliquez sur , cochez la case contre la politique nécessaire et cliquez sur **Appliquer**. Les paramètres du poste seront hérités des paramètres de la version actuelle de cette politique. Vous pouvez assigner au poste une seule politique au maximum.

- Dans la liste **Profil**, vous pouvez spécifier le profil du composant Contrôle des applications qui sera appliqué au poste créé.

Le profil est hérité par défaut du groupe parent du poste. Pour sélectionner le profil pour un poste, cliquez sur **Éditer** , cochez la case contre le profil nécessaire et cliquez sur **Appliquer**. Plusieurs profils peuvent être assignés à un poste.

9. Dans la section **Serveur proxy Dr.Web**, vous pouvez spécifier les paramètres du Serveur proxy Dr.Web lié à ce poste.

Si vous voulez installer le Serveur proxy sur le poste créé, cochez la case **Créer un Serveur proxy Dr.Web lié** et spécifiez les paramètres du Serveur proxy Dr.Web. Les paramètres sont équivalents aux paramètres utilisés lors de la [création du Serveur proxy Dr.Web](#).



Lors de la création du compte du poste, le compte du Serveur proxy Dr.Web sera créé dans le Centre de gestion. Après la transmission des paramètres sur le poste, le Serveur proxy Dr.Web sera installé sur ce poste en tâche de fond. L'Agent Dr.Web se connectera au Serveur Dr.Web uniquement via le Serveur proxy Dr.Web installé. L'utilisation du Serveur proxy Dr.Web sera transparente pour l'utilisateur.

10. Si nécessaire, spécifiez des informations dans la rubrique **Sécurité**. Pour en savoir plus sur la configuration de cette rubrique, consultez le **Manuel Administrateur** dans la rubrique [Sécurité](#).
11. Si nécessaire, spécifiez les paramètres dans la rubrique **Emplacement**.
12. Cliquez sur le bouton **Enregistrer** se trouvant en haut, au coin droit de la fenêtre. Une fenêtre apparaît et informe sur la création réussie du nouveau poste, cette fenêtre affiche également le numéro d'identification et les liens suivants :
 - Dans l'élément **Fichier d'installation** : lien de téléchargement du package d'installation personnel de l'Agent Dr.Web.
 - Dans l'élément **Fichier de configuration** — un lien pour télécharger le fichier contenant les paramètres de connexion au Serveur Dr.Web pour les postes sous OS Android, macOS et Linux.



Immédiatement après la création d'un nouveau poste et jusqu'au moment où un système d'exploitation pour le poste en question ne soit défini, dans la section de téléchargement de la distribution, les liens sont fournis séparément pour chaque OS pris en charge par Dr.Web Enterprise Security Suite.

Les liens de téléchargement du package d'installation personnel de l'Agent Dr.Web et du fichier de configuration sont également disponibles :

- depuis l'élément Propriétés du poste après sa création,



- dans la rubrique **Objets sélectionnés** lors de la sélection du poste créé dans l'arborescence.

Pour obtenir les packages d'installation personnels sous les systèmes d'exploitation autres que Windows, après l'installation du Serveur Dr.Web, il faut télécharger dans le référentiel les produits d'entreprise Dr.Web correspondants se trouvant sur les serveurs du SGM.

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](#).

- L'élément **Mot de passe** contient le mot de passe pour l'accès de ce poste au Serveur Dr.Web. Pour voir le mot de passe, cliquez sur .
 - L'élément **Mot de passe du Serveur proxy** contient le mot de passe pour l'accès du Serveur proxy Dr.Web au Serveur Dr.Web si le poste a été créé avec le Serveur proxy Dr.Web lié (voir l'étape 9).
 - Le bouton **Installer** est réservé pour l'[installation de l'Agent Dr.Web à distance en utilisant le Centre de gestion de la sécurité Dr.Web](#).
13. La marche à suivre pour installer le logiciel de l'Agent Dr.Web est décrite dans le **Manuel Utilisateur** pour les OS correspondants.

Paramètres de connexion au Serveur Dr.Web pour un poste tournant sous macOS

1. Dans le menu de l'application Antivirus Dr.Web, cliquez sur **Paramètres** et sélectionnez la rubrique **Mode**.
2. Cochez la case **Activer le mode de protection centralisée**.
3. De tels paramètres de connexion au Serveur Dr.Web comme l'adresse IP et les paramètres d'authentification sur le Serveur Dr.Web sont spécifiés automatiquement depuis le fichier de configuration `install.cfg` situé à l'intérieur du package d'installation personnel.

Pour utiliser le fichier :

- a) Dans le Gestionnaire de licences cliquez sur **Autres types d'activation**.
- b) Faites un glisser-déposer du fichier contenant les paramètres dans la fenêtre qui s'ouvre ou cliquez sur la zone pointillée pour ouvrir la fenêtre de sélection du fichier.

Après la connexion du fichier, les champs de saisie de paramètres de connexion au Serveur Dr.Web seront remplis automatiquement.

5.2.2.2. Installation de l'Agent Dr.Web avec le package d'installation de groupe

Pour installer l'Agent Dr.Web sur les postes avec le package d'installation de groupe

1. A l'aide du Centre de gestion créez un nouveau groupe utilisateur sur le Serveur Dr.Web (pour en savoir plus sur la procédure de la création de groupes consultez le **Manuel**



Administrateur, p. [Création et suppression de groupes](#)). Vous pouvez également utiliser un groupe existant que vous avez créé précédemment.

2. Si nécessaire, spécifiez dans le Gestionnaire de licence la clé de licence personnelle pour le groupe. Sinon, le groupe va hériter la clé de licence du groupe parent.
3. A l'aide du Centre de gestion [créez des comptes](#) pour de nouveaux postes sur le Serveur Dr.Web. Ajoutez les nouveaux comptes de postes dans le groupe utilisateur de l'étape 1 et spécifiez ce groupe comme primaire. Dans le groupe utilisateur, il est possible de créer autant de nouveaux postes qu'il y a des licences libres disponibles dans ce groupe.
4. Le lien vers le package d'installation de groupe sera disponible dans les paramètres du groupe. Les packages d'installation seront partagés selon les systèmes d'exploitation disponibles : un package d'installation pour chaque système d'exploitation.
5. Si les utilisateurs effectuent l'installation de l'Agent Dr.Web eux-mêmes, envoyez-leur le lien vers le package d'installation de l'Agent Dr.Web pour le système d'exploitation correspondant de l'ordinateur ou de l'appareil mobile. Dans ce cas, le même package d'installation de groupe pour le système d'exploitation correspondant sera envoyé à tous les utilisateurs.
6. Effectuez l'installation de l'Agent Dr.Web sur le poste de travail.



L'installation de l'Agent Dr.Web en mode local sur le poste de travail est décrite dans le **Manuel Utilisateur** pour les OS correspondants.



Les droits d'administrateur sur le poste sont requis pour installer l'Agent Dr.Web.

Si un antivirus est déjà installé sur le poste, avant de procéder à l'installation, l'installateur va essayer de le supprimer. En cas d'échec, l'utilisateur doit désinstaller le logiciel antivirus opérant sur le poste lui-même.

7. Après l'installation de l'Agent Dr.Web, l'Agent Dr.Web se connecte au Serveur Dr.Web indiqué dans le package d'installation de groupe. Lors de la première connexion au Serveur Dr.Web, la disponibilité de postes libres dans le réseau utilisateur, dont le package d'installation a été utilisé pour l'installation de l'Agent Dr.Web. La quantité de postes libres est déterminée d'après le nombre de comptes dans ce groupe dont le délai d'accès n'a pas expiré. A chaque connexion du package d'installation de groupe, le nombre de postes libres est recompté pour fournir des informations actuelles.
 - a) En cas de disponibilité de postes libres. Les paramètres d'authentications de poste pour la connexion au Serveur Dr.Web sont attribués automatiquement. Cette procédure s'effectue de manière transparente pour l'Administrateur et ne nécessite aucune intervention de l'utilisateur.
 - b) En cas d'absence de postes libres dans ce groupe, l'installation s'interrompt et le message adressé à l'utilisateur s'affiche.



5.2.2.3. Installation de l'Agent Dr.Web avec l'installateur

L'installateur de l'Agent Dr.Web se distingue du package d'installation par ce qu'il n'inclut pas les paramètres de connexion au Serveur Dr.Web et les paramètres d'authentification du poste sur le Serveur Dr.Web.

L'installateur de l'Agent Dr.Web et la clé publique de chiffrement sont disponibles depuis la [page d'installation](#) du Centre de gestion de la sécurité Dr.Web.



Pour obtenir les installateurs sous les OS autres que Windows et pour installer la distribution complète de l'installateur sous Windows, il faut télécharger dans le référentiel **Produits d'entreprise Dr.Web** depuis les serveurs du SGM après l'installation du Serveur Dr.Web.

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](#).

Installation en mode local sur les postes tournant sous les OS Android, OS Linux, macOS

L'installateur pour l'installation de l'Agent Dr.Web, équivalent à l'installateur de la version autonome, est disponible pour les postes tournant sous les OS Android, Linux, macOS.



L'installation de l'Agent Dr.Web en mode local sur le poste de travail est décrite dans le **Manuel Utilisateur** pour les OS correspondants.

Si l'installation est effectuée à l'aide de l'installateur sans fichier de configuration, vous serez obligé de spécifier l'adresse du Serveur Dr.Web sur le poste manuellement pour que le poste soit connecté.

Vous pouvez spécifier manuellement ou ne pas spécifier les paramètres d'authentification. Les options suivantes de connexion au Serveur Dr.Web sont possibles :

Variante de tâche	Paramètres d'authentification
Spécifié manuellement	Une tentative d'authentification automatique d'après les paramètres d'authentification s'effectue.
Non spécifié	Le principe d'authentification sur le Serveur Dr.Web dépend des paramètres du Serveur Dr.Web pour la connexion de nouveaux postes (pour en savoir plus, voir Manuel Administrateur , p. Politique d'approbation des nouveaux postes).



Pour spécifier les paramètres d'authentification manuellement, il est nécessaire de créer un nouveau compte du poste dans le Centre de gestion de la Sécurité. Dans ce cas, un [package d'installation](#) contenant un fichier de configuration avec les paramètres de connexion et d'authentification sera disponible. Il est recommandé d'utiliser le package d'installation au lieu de l'installateur.

Installation en mode local sur les postes tournant sous l'OS Windows

Les types suivants des installateurs de l'Agent Dr.Web sont fournis :

- *l'installateur réseau* `drwinst.exe` n'installe que l'Agent Dr.Web. Après la connexion au Serveur Dr.Web, l'Agent Dr.Web télécharge et installe les composants correspondants de ce package antivirus.
- *l'installateur complet* `drweb-<version_de_l'agent>-<assemblage>-esuite-agent-full-windows.exe` effectue l'installation de l'Agent Dr.Web et du package antivirus en même temps.

Lors de l'installation via ces installateurs, vous pouvez ne pas spécifier les paramètres de connexion au Serveur Dr.Web ainsi que les paramètres d'authentification ou vous pouvez les spécifier manuellement.



Pour spécifier les paramètres d'authentification manuellement, il est nécessaire de créer un nouveau compte du poste dans le Centre de gestion de la Sécurité. Dans ce cas, un [package d'installation](#) sera disponible. S'il n'y a pas de nécessité d'installer à l'aide de la distribution complète ou de l'installateur réseau, il est recommandé d'utiliser le package d'installation au lieu de l'installateur.

Les options suivantes de connexion au Serveur Dr.Web sont possibles :

Variante de tâche	Adresse du Serveur Dr.Web	Paramètres d'authentification
Spécifié manuellement	Le poste se connecte directement au Serveur Dr.Web spécifié.	Une tentative d'authentification automatique d'après les paramètres d'authentification s'effectue.
Non spécifié	L'Agent Dr.Web recherche le Serveur Dr.Web dans le réseau en utilisant le <i>Service de détection de Serveur Dr.Web</i> . Une tentative de connexion au premier Serveur Dr.Web trouvé s'effectue.	Le principe d'authentification sur le Serveur Dr.Web dépend des paramètres du Serveur Dr.Web pour la connexion de nouveaux postes (pour en savoir plus, voir Manuel Administrateur , p. Politique d'approbation des nouveaux postes).



Les options de l'installation de l'Agent Dr.Web à l'aide de l'installateur complet et du package d'installation sont décrites dans le **Manuel Utilisateur** pour l'OS Windows.

Il est recommandé que l'installation via l'installateur réseau soit effectuée par l'administrateur du réseau antivirus.

Installation en mode local avec l'installateur réseau sous l'OS Windows

L'installateur réseau de l'Agent Dr.Web `drwinst.exe` est fourni pour l'installation de l'Agent Dr.Web uniquement sur les postes tournant sous Windows.

Si l'installateur réseau a été lancé au cours de l'installation standard (c'est-à-dire sans clé `/instMode remove`) sur un poste sur lequel l'installation avait déjà été effectuée, cela n'entraîne aucune action. L'installateur achève son fonctionnement et affiche une fenêtre avec la liste des clés supportées.

L'installation avec l'installateur réseau peut être effectuée dans deux modes :

1. *Mode Tâche de fond* est lancé si la clé du mode Tâche de fond est spécifiée.
2. *Mode Graphique* est spécifié par défaut. Il est lancé si la clé du mode Tâche de fond n'est pas spécifiée.

Vous pouvez également installer l'Agent Dr.Web sur le poste de manière distante via le Centre de gestion, (voir p. [Installation à distance de l'Agent Dr.Web](#)).

Pour installer l'Agent Dr.Web sur le poste de travail en tâche de fond

1. Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de l'Agent Dr.Web (en cas d'installation du Serveur Dr.Web, c'est le sous-répertoire `webmin/install/windows` dans le répertoire d'installation du Serveur Dr.Web. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et le certificat `drwcsd-certificate.pem` depuis la [page d'installation](#) du Centre de gestion. Lancez le fichier `drwinst.exe` avec la clé du mode de tâche de fond `/silent yes`.

Par défaut, le fichier `drwinst.exe` lancé sans paramètres de connexion au Serveur Dr.Web utilise le mode *Multicast* pour scanner le réseau afin de trouver des Serveurs Dr.Web actifs et tente d'installer l'Agent Dr.Web depuis le premier Serveur Dr.Web trouvé dans le réseau.



En cas d'utilisation du mode *Multicast* pour rechercher les Serveurs Dr.Web actifs, l'installation de l'Agent Dr.Web sera effectuée depuis le premier Serveur Dr.Web trouvé. Dans ce cas, si la clé publique de chiffrement ne correspond pas à la clé de chiffrement du Serveur Dr.Web, l'installation se termine avec une erreur. Si c'est le cas, veuillez spécifier l'adresse du Serveur Dr.Web au démarrage de l'installateur de manière explicite (voir ci-dessous).



S'il faut installer l'Agent Dr.Web sur l'ordinateur sur lequel le Serveur Dr.Web est installé, il faut spécifier l'adresse du Serveur Dr.Web directement dans les paramètres de lancement de l'installateur, car le Serveur Dr.Web risque de ne pas être détecté lors de la recherche via une requête multicast.

Le fichier `drwinst.exe` peut également être lancé avec les paramètres avancés de la ligne de commande suivants :

- Dans le cas où le mode *Multicast* ne serait pas utilisé, lors de l'installation de l'Agent Dr.Web, il est recommandé d'utiliser le nom du Serveur Dr.Web (pré-enregistré dans le service DNS) :

```
drwinst /silent yes /server <nom_DNS_du_Serveur_Dr.Web>
```



En tant qu'adresse du Serveur Dr.Web il est recommandé d'utiliser le nom du Serveur Dr.Web au format FQDN enregistré préalablement dans le service DNS. Cela facilitera le processus de configuration du réseau antivirus relatif à la procédure de réinstallation du Serveur Dr.Web sur un autre ordinateur. Dans ce cas, si vous voulez changer l'adresse du Serveur Dr.Web, il suffira de la changer dans les paramètres du serveur DNS pour le nom de l'ordinateur hébergeant le Serveur Dr.Web. Tous les agents se connecteront automatiquement au nouveau serveur.

1. Si le serveur DNS local fonctionne dans le réseau, il faut y créer un nom à part pour le Serveur Dr.Web et pour le Serveur proxy Dr.Web (par exemple, `drwebes.company.lan`).
2. Dans les paramètres des Agents Dr.Web, il faut indiquer le nom du Serveurs Dr.Web au format FQDN.
3. En plus du nom au format FQDN, il est recommandé d'ajouter dans les paramètres de l'Agent Dr.Web l'adresse du Serveur Dr.Web et maintenir cette adresse à jour en cas de son changement. Dans ce cas, s'il est impossible d'utiliser le nom du serveur, l'agent tentera de se connecter par l'adresse du serveur.

- Vous pouvez aussi spécifier l'adresse du Serveur Dr.Web de façon explicite, par exemple :

```
drwinst /silent yes /server 192.168.1.3
```

- L'utilisation de la clé `/regagent yes` permet d'enregistrer l'Agent Dr.Web lors de l'installation dans la liste d'ajout/suppression de programmes.



Vous pouvez consulter la liste complète des paramètres de l'Installateur réseau dans le document **Annexes**, [G1. Installateur réseau](#).

2. Lorsque l'installation est finie, le logiciel de l'Agent Dr.Web est installé sur le poste (ce n'est pas le package antivirus).
3. Dès que le poste est approuvé sur le Serveur Dr.Web (dans le cas où l'approbation est requise par la configuration du Serveur Dr.Web), le package antivirus sera automatiquement installé.



4. Redémarrez l'ordinateur selon la requête de l'Agent Dr.Web.

Pour installer l'Agent Dr.Web sur le poste en mode graphique

Sur le poste sur lequel vous souhaitez installer l'antivirus, ouvrez le répertoire réseau d'installation de l'Agent Dr.Web (en cas d'installation du Serveur Dr.Web, c'est le sous-répertoire `webmin/install/windows` dans le répertoire d'installation du Serveur Dr.Web. Vous pourrez le déplacer ultérieurement) ou téléchargez le fichier exécutable de l'installateur `drwinst.exe` et le certificat `drwcsd-certificate.pem` depuis la [page d'installation](#) du Centre de gestion. Lancez le fichier `drwinst.exe`.

La fenêtre de l'assistant d'installation de l'Agent Dr.Web va s'ouvrir. Les actions suivantes pour installer l'Agent Dr.Web sur le poste à l'aide de l'installateur réseau en mode graphique sont équivalentes aux actions d'installation à l'aide du package d'installation, mais sans paramètres de connexion au Serveur Dr.Web, s'ils n'ont pas été spécifiés dans la clé correspondante de la ligne de commande.



L'installation de l'Agent Dr.Web sur les postes de travail est décrite dans le manuel **Agent Dr.Web pour Windows. Manuel Utilisateur**.

5.2.3. Installation de l'Agent Dr.Web à distance

Dr.Web Enterprise Security Suite permet de détecter les ordinateurs sur lesquels la protection antivirus Dr.Web Enterprise Security Suite n'a pas encore été installée et dans certains cas, il permet également d'installer cette protection à distance.

L'installation à distance peut être effectuée :

- [Via le Centre de gestion](#).
- [Avec le service Active Directory](#), si ce service est utilisé dans le réseau local protégé.



L'installation des Agents Dr.Web à distance n'est possible que sur les postes tournant sous Linux ou un OS de la famille Windows (voir [Pré-requis système](#)), sauf les éditions Starter et Home.

Les droits d'administrateur pour les postes sont requis pour pouvoir installer à distance l'Agent Dr.Web sur ces postes.

5.2.3.1. Installation de l'Agent Dr.Web via le Centre de gestion de la sécurité Dr.Web

- [Installation à distance de l'Agent Dr.Web sous Windows](#)
- [Installation de l'Agent Dr.Web à distance sous les OS UNIX](#)



5.2.3.1.1. Installation à distance de l'Agent Dr.Web sous Windows

Il existe des méthodes suivantes d'installation à distance des Agents Dr.Web sur les postes de travail au sein du réseau :

1. [Installation avec le Scanner réseau.](#)

Permet d'effectuer une recherche préliminaire des ordinateurs non protégés dans le réseau et d'installer sur tels ordinateurs les Agents Dr.Web.

2. [Installation avec l'outil Installation via réseau.](#)

A choisir dans le cas où vous connaissez l'adresse du poste ou du groupe des postes sur lesquels seront installés les Agents Dr.Web.

3. [Installation sur les postes avec les ID spécifiés.](#)

Permet d'installer sur les postes et vers les groupes des postes des Agents Dr.Web pour les comptes sélectionnés (y compris tous les nouveaux comptes existants) avec les ID spécifiés et les mots de passe pour accéder au Serveur Dr.Web.



Pour le bon fonctionnement du Scanner réseau et de l'outil **Installation via réseau** sous le navigateur Windows Internet Explorer, l'adresse IP ou/et le nom DNS de l'ordinateur sur lequel est installé le Serveur Dr.Web doivent être ajoutés aux sites de confiance du navigateur dans lequel est ouvert le Centre de gestion Sécurité pour l'installation à distance.

Utilisation du Scanner réseau

L'arborescence du réseau antivirus affichée dans le Centre de gestion contient les ordinateurs déjà inclus dans le réseau antivirus. Dr.Web Enterprise Security Suite permet également de détecter les ordinateurs non protégés par l'antivirus Dr.Web Enterprise Security Suite, et d'installer à distance des composants antivirus.

Afin d'effectuer une installation rapide du logiciel de l'Agent Dr.Web sur les postes de travail, il est recommandé d'utiliser le Scanner réseau (voir **Guide d'installation**, p. [VScanner réseau](#)) qui recherche les postes par leurs adresses IP.



L'installation via le réseau est disponible uniquement pour les administrateurs possédant le droit **Voir les propriétés des groupes de postes**, fourni pour tout le réseau antivirus (en savoir plus sur les droits d'administrateurs, voir le **Manuel Administrateur**, [Droits d'administrateurs](#)).

Pour installer l'Agent Dr.Web avec le Scanner réseau


1. Ouvrez le Scanner réseau. Pour ce faire, sélectionnez l'élément **Administration** dans le menu principal du Centre de gestion. Dans la fenêtre qui apparaît sélectionnez l'élément du menu de gestion **Scanner réseau**. Une fenêtre vide portant le même nom s'ouvrira.




- Spécifiez les paramètres de recherche des postes sur le réseau. Pour une description détaillée des paramètres, consultez le **Manuel Administrateur**, p. [Scanner réseau](#).
- Cliquez sur le bouton **Scanner**. L'arborescence dans laquelle il est indiqué pour chaque poste si l'antivirus est installé ou pas sera téléchargée dans la fenêtre.
- Ouvrez les éléments de l'arborescence correspondant aux groupes de travail (domaines). Tous les éléments de l'arborescence correspondant aux divers groupes de travail et aux postes sont marqués par les icônes dont vous trouverez la description ci-dessous.

Tableau 5-1. Apparence des icônes

icône	Description
Groupes de travail	
	Groupes de travail contenant entre autres les ordinateurs sur lesquels l'antivirus Dr.Web Enterprise Security Suite peut être installé.
	Groupes restants contenant les ordinateurs sur lesquels l'antivirus est déjà installé ou les ordinateurs inaccessibles via le réseau.
Postes de travail	
	Postes actif avec l'antivirus installé.
	Poste actif avec le statut non approuvé du logiciel : il n'y a pas de logiciel antivirus sur l'ordinateur ou la disponibilité de l'antivirus n'est pas vérifiée.

Vous pouvez ouvrir les éléments du répertoire correspondant aux postes ayant l'icône  pour consulter l'ensemble des composants installés.

- Dans la fenêtre du **Scanner réseau**, sélectionnez un ordinateur non protégé (ou plusieurs ordinateurs non protégés en utilisant les boutons CTRL ou SHIFT).
- Dans la barre d'outils, cliquez sur le bouton  **Installer l'Agent Dr.Web**.
- La fenêtre **Installation via réseau** va s'afficher pour créer la tâche d'installation de l'Agent Dr.Web.
- Dans le champ **Adresses des postes**, spécifiez les adresses IP ou les noms DNS des ordinateurs sur lesquels vous souhaitez installer l'Agent Dr.Web. Si vous spécifiez plusieurs adresses, utilisez « ; » ou « , » pour les séparer (le nombre d'espaces n'a pas d'importance).
En cas d'installation sur les postes trouvés avec le Scanner Réseau, l'adresse du poste ou des plusieurs postes sur lesquels sera effectuée l'installation sera indiquée dans le champ **Adresses des postes**.



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes, Annexe D. Spécification de l'adresse réseau**.

- Par défaut, dans le champ **Serveur Dr.Web**, s'affiche l'adresse IP ou le nom DNS du Serveur Dr.Web auquel le Centre de gestion est connecté. Si nécessaire, spécifiez dans ce champ l'adresse du Serveur Dr.Web depuis lequel le logiciel antivirus sera installé. Utilisez « ; » ou



« , » pour séparer plusieurs Serveurs Dr.Web (le nombre d'espaces avant et après le séparateur n'a pas d'importance). Laissez le champ vide pour utiliser le service de détection du Serveur Dr.Web (mode *Multicast*).



L'installation distante de l'Agent Dr.Web n'est pas disponible sur l'ordinateur avec le Serveur Dr.Web installé depuis lequel est lancée l'installation.



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).

Lors de l'installation de l'Agent Dr.Web, il est recommandé d'utiliser le nom du Serveur Dr.Web au [format FQDN](#) en tant qu'adresse du Serveur Dr.Web.

10. Dans le champ **Nombre des installations simultanées**, spécifiez le nombre maximum des postes sur lesquels l'installation distante est possible.
11. Cochez la case **Installer le logiciel Agent Dr.Web pour Windows** pour spécifier les paramètres spécifiques pour l'installation à distance sous Windows.
12. Par défaut, le logiciel de l'Agent Dr.Web sera installé sur le poste, dans le répertoire `C:\Program Files\DrWeb`. Si nécessaire, vous pouvez spécifier un autre chemin dans le champ **Répertoire d'installation de l'Agent Dr.Web**.
Il est recommandé de spécifier le chemin complet pour la détermination exacte de l'emplacement du répertoire d'installation. Lors de la spécification, les variables d'environnement peuvent être utilisées.
13. Dans le menu déroulant **Langue**, sélectionnez la langue de l'interface de l'Antivirus Dr.Web qui sera installé sur les postes.
14. Dans le champ **Délai d'installation (s)**, spécifiez un délai d'attente maximum en secondes avant la fin d'installation de l'Agent Dr.Web. Les valeurs possibles sont les suivantes : 1–600. Le délai de 180 secondes est spécifié par défaut. En cas de faible bande passante de la connexion entre le Serveur Dr.Web et l'Agent Dr.Web, il est recommandé d'augmenter la valeur spécifiée par défaut.




En cas de grande quantité de données, le délai d'installation peut dépasser la durée de la session. Si la durée de la session s'écoule avant la fin de l'installation, le processus sera automatiquement arrêté et l'Agent Dr.Web ne sera pas installé.

15. Si nécessaire, cochez la case **Enregistrer l'Agent Dr.Web dans la liste des logiciels installés**.
16. Dans la rubrique **Composants à installer**, sélectionnez les composants du package antivirus à installer sur les postes.
17. Dans les rubriques **Compression** et **Chiffrement**, spécifiez les paramètres de la compression et du chiffrement utilisés par l'Installateur réseau lors de l'installation de l'Agent Dr.Web et du package antivirus. Ces paramètres seront également utilisés pour l'interaction entre l'Agent Dr.Web et le Serveur Dr.Web lors de l'installation.



18. Dans la rubrique **Authentification sur les postes distants**, spécifiez les paramètres d'authentification nécessaires pour accéder aux postes distants sur lesquels l'Agent Dr.Web sera installé :

- **Utilisateur** : nom d'utilisateur pour l'authentification sur les postes sur lesquels l'installation distante sera effectuée. Pour les utilisateurs de domaine, il faut indiquer le nom de domaine au format `<domaine>\<utilisateur>` ou `<utilisateur>@<domaine>`. Pour les utilisateurs locaux, il faut indiquer le nom de poste ou le nom de groupe de travail au format `<poste>\<utilisateur>` ou `<groupe>\<utilisateur>`.
- **Mot de passe** : mot de passe d'utilisateur sur le poste distant.

Il est possible de spécifier plusieurs comptes administrateur. Pour ajouter encore un compte, cliquez sur  et remplissez les champs relatifs à l'authentification. De façon analogique pour chaque nouvelle entrée.

Lors de l'installation de l'Agent Dr.Web, c'est le premier compte de la liste qui est utilisé en premier lieu. Si l'installation sous ce compte a échoué, le compte suivant sera utilisé, etc.

19. Dans la section **Paramètres de redémarrage**, cochez la case **Redémarrer le poste** et spécifiez l'heure et la période de redémarrage dans la liste déroulante (y compris tout de suite après l'installation de l'Agent Dr.Web).

- **Tout de suite après l'installation** : le poste sera redémarré tout de suite après l'installation de l'Agent Dr.Web.
- **À l'heure spécifiée** : conformément à l'heure du système dans lequel l'administrateur a lancé le navigateur et a spécifié le paramètre.
- **Pendant la période spécifiée** : conformément à l'heure locale sur le poste.

20. Après avoir spécifié tous les paramètres nécessaires, cliquez sur le bouton **Installer**.



Un service intégré est utilisé pour lancer l'installation de l'antivirus.

Pour lancer l'installation, on utilise l'installateur réseau du Serveur Dr.Web actuel se trouvant dans le répertoire `webmin\install\windows` du répertoire d'installation du Serveur Dr.Web et le certificat SSL `drwcsd-certificate.pem` se trouvant dans le répertoire `etc` du répertoire d'installation du Serveur Dr.Web.

Si les packages d'installation pour l'installation distante de l'Agent Dr.Web sont introuvables dans le référentiel du Serveur Dr.Web, contactez le support technique de Doctor Web : <https://support.drweb.com/>.

21. L'Agent Dr.Web sera installé sur les postes spécifiés. Après l'approbation du poste sur le Serveur Dr.Web (si l'approbation est requise selon la configuration du Serveur Dr.Web, voir aussi le **Manuel administrateur** p. [Politique de connexion des postes](#)), le package antivirus sera installé de manière automatique.

22. Redémarrez l'ordinateur selon la requête de l'Agent Dr.Web. **Utilisation de l'outil Installation via réseau**



Lorsque le réseau antivirus est créé et qu'il faut installer l'Agent Dr.Web sur les postes particuliers, il est recommandé d'utiliser l'**Installation via réseau**.



L'installation via le réseau est disponible uniquement pour les administrateurs possédant le droit **Voir les propriétés des groupes de postes**, fourni pour tout le réseau antivirus (en savoir plus sur les droits d'administrateurs, voir le **Manuel Administrateur**, [Droits d'administrateurs](#)).

Pour installer l'Agent Dr.Web via le réseau

1. Dans le menu principal, sélectionnez l'élément **Administration**, ensuite, dans le menu de gestion, sélectionnez **Installation via le réseau**.
2. Les étapes suivantes sont équivalentes aux étapes **8–22** de la procédure [ci-dessus](#).

Installation pour les comptes avec les ID spécifiés

En cas de création d'un nouveau compte de poste :

1. Créez un nouveau compte ou plusieurs comptes pour les postes de travail (voir [Création d'un nouveau compte](#)).
2. Immédiatement après la création du compte, dans la partie droite de la fenêtre principale, le panneau au titre **Créer un poste** va s'afficher. Cliquez sur **Installer**.
3. La fenêtre du Scanner réseau va s'afficher.
4. Les étapes suivantes sont équivalentes aux étapes **2–22** de la procédure [ci-dessus](#).
5. Après la fin de l'installation, vérifiez que les [icônes](#) se trouvant contre les postes en question dans l'arborescence ont été changées.

En cas d'utilisation d'un compte de poste existant :

1. Dans l'arborescence du réseau antivirus, sélectionnez un nouveau poste ou un groupe des postes pour lesquels les Agents Dr.Web n'ont pas encore été installés, vous pouvez également sélectionner le groupe **New** (pour l'installation vers tous les nouveaux comptes).
2. Dans la barre d'outils, cliquez sur le bouton **Installer l'Agent Dr.Web**.
3. La fenêtre du Scanner réseau va s'afficher.
4. Les étapes suivantes sont équivalentes aux étapes **2–22** de la procédure [ci-dessus](#).
5. Après la fin de l'installation, vérifiez que les [icônes](#) se trouvant contre les postes en question dans l'arborescence ont été changées.



L'installation de l'Agent Dr.Web sur les postes avec les ID sélectionnées est également disponible pour l'administrateur des groupes.



En cas d'erreurs lors de l'installation à distance, consultez la rubrique **Annexes** [Diagnostic des problèmes d'installation à distance](#).

Configuration supplémentaire

- Si les postes de travail font partie du domaine et que le compte administrateur de domaine est utilisé pour l'installation, il est nécessaire d'activer le partage de fichiers et d'imprimantes sur les postes. Pour savoir l'emplacement du paramètre sous différentes versions de Windows, consultez le [tableau](#).
- Si les postes du réseau n'appartiennent pas au domaine ou que le compte local est utilisé pour l'installation, une configuration supplémentaire de postes sera nécessaire sous certaines versions de Windows.

Configuration supplémentaire en cas d'installation à distance vers un poste se trouvant hors du domaine ou en cas d'utilisation du compte local



Les paramètres en question peuvent affaiblir le niveau de protection des ordinateurs du réseau. Il est fortement recommandé de prendre connaissance de l'utilisation de ces paramètres avant d'apporter des modifications dans le système ou de refuser l'installation à distance et d'installer l'Agent Dr.Web [manuellement](#).

Après la configuration du poste de réseau, il est recommandé de réinitialiser tous les paramètres modifiés et de reprendre les valeurs initiales pour ne pas bousculer la politique de base du système d'exploitation.

En cas d'installation à distance de l'Agent Dr.Web sur un poste se trouvant hors du domaine et/ou en cas d'utilisation du compte local, réalisez les actions suivantes sur l'ordinateur sur lequel sera installé l'Agent Dr.Web :

OS	Configuration	
Windows XP	Configurez le mode d'accès aux fichiers partagés	Nouveau style : Démarrer → Configuration → Panneau de configuration → Apparence et thèmes → Options des dossiers → Onglet Affichage → Décochez la case Utiliser le partage de fichiers simple (recommandé)
		Style classique : Démarrer → Configuration → Panneau de configuration → Options des dossiers → Onglet Affichage → Décochez la case Utiliser le partage de fichiers simple (recommandé)



OS	Configuration	
	Configurez le mode d'authentification réseau dans les stratégies locales	<p>Nouveau style :</p> <p>Démarrer → Configuration → Panneau de configuration → Performances et maintenance → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p> <p>Style classique :</p> <p>Démarrer → Configuration → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Options de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p>
	Désactiver Windows Firewall sur le poste avant l'installation à distance.	
Windows Server 2003	Désactiver Windows Firewall sur le poste avant l'installation à distance.	
Windows Vista Windows Server 2008	Activer le partage de fichiers	<p>Nouveau style :</p> <p>Démarrer → Configuration → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Partage et découverte → Partage de fichiers → Activer.</p> <p>Style classique :</p> <p>Démarrer → Configuration → Panneau de configuration → Centre Réseau et partage → Partage et découverte → Partage de fichiers → Activer.</p>
	Configurez le mode d'authentification réseau dans les stratégies locales	<p>Nouveau style :</p> <p>Démarrer → Configuration → Panneau de configuration → Système et maintenance → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p> <p>Style classique :</p> <p>Démarrer → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p>



OS	Configuration	
	<p>Créer la clé LocalAccountTokenFilterPolicy :</p> <ol style="list-style-type: none">Dans l'éditeur d'enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l'enregistrement LocalAccountTokenFilterPolicy n'existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.Dans le menu contextuel de l'élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK. <p>Le redémarrage n'est pas requis.</p>	
Windows 7 Windows Server 2008 R2	Activer le partage de fichiers et d'imprimantes	<p>Nouveau style :</p> <p>Démarrer → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</p> <p>Style classique :</p> <p>Démarrer → Panneau de configuration → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</p>
	Configurez le mode d'authentification réseau dans les stratégies locales	<p>Nouveau style :</p> <p>Démarrer → Panneau de configuration → Système et sécurité → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p> <p>Style classique :</p> <p>Démarrer → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p>
	<p>Créer la clé LocalAccountTokenFilterPolicy :</p> <ol style="list-style-type: none">Dans l'éditeur d'enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l'enregistrement LocalAccountTokenFilterPolicy n'existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.	



OS	Configuration	
	<p>b) Dans le menu contextuel de l'élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.</p> <p>c) Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK.</p> <p>Le redémarrage n'est pas requis.</p>	
Windows 8 Windows 8.1 Windows Server 2012	Activer le partage de fichiers et d'imprimantes	<p>Nouveau style :</p> <p>Paramètres → Panneau de configuration → Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</p>
Windows Server 2012 R2		<p>Style classique :</p> <p>Paramètres → Panneau de configuration → Centre Réseau et partage → Modifier les paramètres de partage avancés → Partage de fichiers et d'imprimantes → Activer le partage de fichiers et d'imprimantes.</p>
Windows 10		
	Configurez le mode d'authentification réseau dans les stratégies locales	<p>Nouveau style :</p> <p>Paramètres → Panneau de configuration → Système et sécurité → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p>
		<p>Style classique :</p> <p>Paramètres → Panneau de configuration → Outils d'administration → Stratégie de sécurité locale → Paramètres de sécurité → Stratégies locales → Paramètres de sécurité → Accès réseau : modèle de partage et de sécurité pour les comptes locaux → Classique – les utilisateurs locaux s'authentifient eux-mêmes.</p>
	<p>Créer la clé LocalAccountTokenFilterPolicy :</p> <p>a) Dans l'éditeur d'enregistrement, ouvrez la branche HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Si l'enregistrement LocalAccountTokenFilterPolicy n'existe pas, dans le menu Editer, sélectionnez Ajouter et indiquez la valeur DWORD. Entrez la valeur LocalAccountTokenFilterPolicy et cliquez sur ENTRER.</p> <p>b) Dans le menu contextuel de l'élément LocalAccountTokenFilterPolicy, sélectionnez Modifier.</p> <p>c) Dans le champ Valeur, indiquez la valeur 1 et cliquez sur OK.</p> <p>Le redémarrage n'est pas requis.</p>	



Si le compte se trouvant sur un poste de réseau a un mot de passe vierge, spécifiez dans les politiques locales une stratégie d'accès avec un mot de passe vierge : **Panneau de configuration** → **Outils d'administration** → **Stratégie de sécurité locale** → **Paramètres de sécurité** → **Stratégies locales** → **Options de sécurité** → **Comptes : restreindre l'utilisation de mots de passe vierge par le compte local à l'ouverture de session console** → **Désactiver**.

5.2.3.1.2. Installation de l'Agent Dr.Web à distance sous les OS UNIX

Avant le début de l'installation :

1. Configurez l'accès via SSH depuis l'ordinateur sur lequel le Serveur Dr.Web est installé à l'ordinateur sur lequel l'Agent Dr.Web sera installé (l'installation à distance est effectuée par SSH).
2. Dans la section **Configuration générale du référentiel** du Centre de gestion, sélectionnez les packages de l'Agent Dr.Web pour UNIX à télécharger. Pour ce faire, sélectionnez l'élément **Administration** du menu principal. Ensuite dans le menu de gestion, sélectionnez **Configuration générale du référentiel**. Dans la section **Packages d'installation Dr.Web**, sélectionnez l'onglet **Produits d'entreprise Dr.Web**, ensuite **Dr.Web pour Linux**. Sélectionnez la plateforme nécessaire.



Téléchargez les packages pour les plateformes qui sont nécessaires et que vous utilisez. Le téléchargement de tous les packages demande du temps et de l'espace supplémentaire sur le disque.

3. Téléchargez les packages de l'Agent Dr.Web pour UNIX dans le référentiel. Deux fois par heure ils se téléchargent eux-mêmes selon la planification du Planificateur de tâches. Sinon, effectuez une mise à jour forcée du référentiel. Pour ce faire, sélectionnez l'élément **Administration** du menu principal, ensuite, dans le menu de gestion, sélectionnez **Statut du référentiel**, puis **Vérifier les mises à jour**.

Pour vérifier le téléchargement des packages de l'Agent Dr.Web pour UNIX, sélectionnez l'élément **Administration** du menu principal, ensuite, dans le menu de gestion, sélectionnez **Produits d'entreprise**.

Ensuite, vous pouvez commencer l'installation.

Pour l'installation à distance de l'Agent Dr.Web sur les ordinateurs tournant sous l'OS de la famille UNIX, utilisez l'outil Installation via le réseau dans le Centre de gestion de la sécurité Dr.Web.



Lors de l'installation de l'Agent Dr.Web sur le poste, un répertoire est créé sur le poste. Ce répertoire contient la distribution et le journal d'installation. Le chemin d'accès à ce répertoire est indiqué dans l'interface Web au démarrage de l'installation (le paramètre **Répertoire de fichiers temporaires**).



Pour installer l'Agent Dr.Web via le réseau

1. Dans le menu principal, sélectionnez l'élément **Administration**, ensuite, dans le menu de gestion, sélectionnez **Installation via le réseau**.
2. Dans le champ **Adresses des postes**, spécifiez les adresses IP ou les noms DNS des ordinateurs sur lesquels vous souhaitez installer l'Agent Dr.Web. Si vous spécifiez plusieurs adresses, utilisez « ; » ou « , » pour les séparer (le nombre d'espaces n'a pas d'importance).



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).

3. Par défaut, dans le champ **Serveur Dr.Web**, s'affiche l'adresse IP ou le nom DNS du Serveur Dr.Web auquel le Centre de gestion est connecté. Si nécessaire, spécifiez dans ce champ l'adresse du Serveur Dr.Web depuis lequel le logiciel antivirus sera installé. Utilisez « ; » ou « , » pour séparer plusieurs Serveurs Dr.Web (le nombre d'espaces avant et après le séparateur n'a pas d'importance). Laissez le champ vide pour utiliser le service de détection du Serveur Dr.Web (mode *Multicast*).



L'installation distante de l'Agent Dr.Web n'est pas disponible sur l'ordinateur avec le Serveur installé depuis lequel l'installation est lancée.



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, dans la rubrique [Annexe D. Spécification de l'adresse réseau](#).

Lors de l'installation de l'Agent Dr.Web, il est recommandé d'utiliser le nom du Serveur Dr.Web au [format FQDN](#) en tant qu'adresse du Serveur Dr.Web.

4. Dans le champ **Nombre des installations simultanées**, spécifiez le nombre maximum des postes sur lesquels l'installation distante est possible.
5. Cochez la case **Installer le logiciel Agent Dr.Web pour UNIX** pour spécifier les paramètres spécifiques pour l'installation à distance sous l'OS de la famille UNIX.
6. Dans le champ **Délai de connexion et d'authentification (s)**, spécifiez le délai d'attente maximal de la connexion et de l'authentification sur les postes distants (en secondes).
7. Dans le champ **Délai de transmission des packages d'installation (s)**, spécifiez le délai d'attente maximal de la fin de transmission des packages d'installation (en secondes).
8. Dans le champ **Délai d'installation de packages (s)**, spécifiez le délai maximum d'attente de la fin d'installation des packages (en secondes).




En cas de grande quantité de données, le délai d'installation peut dépasser la durée de la session. Si la durée de la session s'écoule avant la fin de l'installation, le processus sera automatiquement arrêté et les packages ne seront pas installés.

9. S'il est nécessaire d'installer le produit Dr.Web pour les serveurs de fichiers UNIX à la place de l'Agent Dr.Web, cochez la case **Installer Dr.Web pour les serveurs de fichiers UNIX**.



10. Dans la rubrique **Connexion aux postes distants via SSH avec un mot de passe**, spécifiez les paramètres d'authentification nécessaires pour accéder aux postes distants sur lesquels l'Agent Dr.Web sera installé :


- **Utilisateur** : nom d'utilisateur pour l'authentification sur les postes sur lesquels l'installation distante sera effectuée. Pour les utilisateurs de domaine, il faut indiquer le nom de domaine au format `<domaine>\<utilisateur>` ou `<utilisateur>@<domaine>`. Pour les utilisateurs locaux, il faut indiquer le nom de poste ou le nom de groupe de travail au format `<poste>\<utilisateur>` ou `<groupe>\<utilisateur>`.
- **Mot de passe** : mot de passe d'utilisateur sur le poste distant.

Il est possible de spécifier plusieurs comptes d'authentification. Pour ajouter encore un compte, cliquez sur  et remplissez les champs relatifs à l'authentification.

Lors de l'installation de l'Agent Dr.Web, les comptes de la liste seront utilisés à tour de rôle. Si l'installation sous un compte a échoué, le compte suivant sera utilisé, etc.

11. Dans la section **Connexion aux postes distants via SSH avec des clés SSH**, vous pouvez spécifier les paramètres d'authentification alternative sur les ordinateurs distants avec l'utilisation des clés de chiffrement :


- **Utilisateur** : nom d'utilisateur pour l'authentification sur les postes sur lesquels l'installation distante sera effectuée. Pour les utilisateurs de domaine, il faut indiquer le nom de domaine au format `<domaine>\<utilisateur>` ou `<utilisateur>@<domaine>`. Pour les utilisateurs locaux, il faut indiquer le nom de poste ou le nom de groupe de travail au format `<poste>\<utilisateur>` ou `<groupe>\<utilisateur>`.
- **Clé SSH publique** : chemin d'accès au fichier de la clé SSH publique.
- **Clé SSH privée** : chemin d'accès au fichier de la clé SSH privée.
- **Mot de passe de la clé SSH privée** : mot de passe de la clé SSH privée (non obligatoire).

Comme dans la section **Connexion aux postes distants via SSH avec un mot de passe**, il existe la possibilité de spécifier plusieurs comptes en même temps. Pour ce faire, il faut cliquer sur le bouton  et remplir les champs correspondants.




Si les paramètres d'authentification de deux sections **Connexion aux postes distants via SSH avec un mot de passe** et **Connexion aux postes distants via SSH avec des clés SSH** sont configurés, ce sont les paramètres d'authentification par les clés de chiffrement qui seront utilisés les premiers pour l'installation de l'Agent Dr.Web.

12. La section **Privilèges de super-utilisateur** contient les paramètres pour l'augmentation des privilèges de l'utilisateur sur un ordinateur distant jusqu'au niveau nécessaire pour l'installation de l'Agent Dr.Web.

- Cochez la case **Utiliser la commande sudo** ou **Utiliser la commande su** pour augmenter les privilèges jusqu'au niveau de `root` lors de l'installation de l'Agent Dr.Web.
- Dans le champ **Délai de saisie du mot de passe (s)**, indiquez le délai maximum de saisie du mot de passe pour l'utilisation de la commande `su` ou `sudo` en secondes.
- Dans le champ **Mot de passe su/sudo**, entrez le mot de passe pour l'utilisation de la commande `su` ou `sudo`. En cliquant sur le bouton , vous pouvez spécifier plusieurs mots



de passe qui seront parcourus successivement. Si vous laissez le champ vide, mais que vous spécifiez le mot de passe de l'utilisateur dans la section **Connexion aux postes distants via SSH avec un mot de passe**, une tentative d'exécuter la commande avec l'utilisation de ce mot de passe aura lieu.

13. Dans le champ **Port** de la section **Paramètres de connexion**, indiquez le numéro du port SSH qui sera utilisé sur les ordinateurs pour l'installation à distance de l'Agent Dr.Web. En utilisant le bouton , vous pouvez indiquer plusieurs ports.
14. Après avoir indiqué tous les paramètres nécessaires, cliquez sur le bouton **Installer**.
15. L'Agent Dr.Web sera installé sur les postes spécifiés. Après l'approbation du poste sur le Serveur Dr.Web (si l'approbation est requise selon la configuration du Serveur Dr.Web, voir aussi le **Manuel administrateur** [Politique de connexion des postes](#)), le package antivirus sera installé de manière automatique.
16. Redémarrez les ordinateurs distants selon la requête de l'Agent Dr.Web.

5.2.3.2. Installation de l'Agent Dr.Web avec le service Active Directory

Si le service **Active Directory** est utilisé dans le réseau local protégé, vous pouvez installer l'Agent Dr.Web sur les postes de manière distante.



Il est possible d'installer l'Agent Dr.Web via Active Directory en utilisant le système de fichiers distribué DFS (voir les **Annexes**, [Utilisation de DFS lors de l'installation de l'Agent Dr.Web via Active Directory](#)).

Installation de l'Agent Dr.Web

Pour installer l'Agent Dr.Web avec le service Active Directory

1. Téléchargez l'installateur de l'Agent Dr.Web pour les réseaux avec **Active Directory** depuis la [page d'installation](#).
2. Depuis le serveur du réseau local supportant le service **Active Directory**, exécutez l'installation de l'Agent Dr.Web en mode administrateur. L'installation peut être réalisée en mode de ligne de commande (**A**), ainsi qu'en mode graphique de l'installateur (**B**).



Lors de la mise à jour du Serveur Dr.Web, la mise à jour de l'installateur de l'Agent Dr.Web pour les réseaux avec Active Directory n'est pas obligatoire. Après la mise à jour du logiciel du Serveur Dr.Web, les Agents Dr.Web et le logiciel antivirus sur les postes seront mis à jour automatiquement après l'installation.



(A) Configuration de l'installation de l'Agent Dr.Web en mode de ligne de commande

Exécutez la commande suivante accompagnée de tous les paramètres nécessaires et du paramètre obligatoire de désactivation du mode graphique /qn :

```
msiexec /a <nom_du_package>.msi /qn [<paramètres>]
```

La clé /a lance le déploiement du package administrateur.

Nom du package

Le nom du package d'installation de l'Agent Dr.Web pour les réseaux avec **Active Directory** est dans la plupart des cas présenté au format suivant :

```
drweb-<version_du_package>-<assemblage>-esuite-agent-activedirectory.msi
```

Paramètres

/qn : paramètre de désactivation du mode graphique. En cas d'utilisation de cette clé, les paramètres ci-dessous sont obligatoires à spécifier :

- **ESSERVERADDRESS=<nom_DNS>** : l'adresse du Serveur Dr.Web auquel l'Agent Dr.Web va se connecter. Pour en savoir plus sur les formats possibles, consultez les **Annexes**, [Annexe D. Spécification de l'adresse réseau](#).
- **ESSERVERPATH=<nom_complet_du_fichier>** : le chemin complet vers le certificat du Serveur Dr.Web et le nom de fichier (par défaut c'est le fichier `drwcsd-certificate.pem` dans le sous-répertoire `webmin/install` du répertoire d'installation du Serveur Dr.Web).
- **TARGETDIR** : le répertoire réseau destiné pour une image de l'Agent Dr.Web (package d'installation modifié de l'Agent Dr.Web), ce répertoire peut être sélectionné depuis l'éditeur des politiques de groupes pour l'installation spécifiée. Le répertoire doit avoir les droits en lecture et en écriture. Le chemin vers le répertoire doit être spécifié au format d'adresses réseau même si le répertoire se trouve sur la machine locale ; ce répertoire doit être accessible depuis les postes ciblés.



Avant l'installation en mode administrateur, il ne faut pas placer manuellement les fichiers pour l'installation dans le répertoire cible pour l'image de l'Agent Dr.Web (voir le paramètre TARGETDIR). L'installateur de l'Agent Dr.Web pour les réseaux avec Active Directory (<nom_du_package>.msi) et les autres fichiers requis pour l'installation des Agents Dr.Web sur les postes de travail seront placés automatiquement dans le répertoire cible lors de l'installation en mode administrateur. Si avant l'installation en mode administrateur, le répertoire cible contient déjà ces fichiers, par exemple, ils sont restés des installations précédentes, les fichiers portant le même nom seront réécrits.

S'il est nécessaire d'effectuer l'installation en mode administrateur depuis les Serveurs Dr.Web différents, il est recommandé de spécifier les répertoires différents pour chaque Serveur Dr.Web.



Après le déploiement du package administrateur, le répertoire `<répertoire_cible>\Program Files\DrWeb` ne doit contenir que le fichier `README.txt`.

Exemples

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\win_serv\drwcs_inst\drwcsd-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem" TARGETDIR=\\comp\share
```

Les mêmes paramètres peuvent être spécifiés dans le mode graphique de l'installateur.

Puis il est nécessaire de spécifier l'installation du package (voir la description de la procédure [ci-dessous](#)) sur le serveur du réseau local sur lequel est installé le logiciel de gestion du service Active Directory.

(B) Configuration de l'installation de l'Agent Dr.Web en mode graphique



Avant l'installation en mode administrateur, veuillez vous assurer que le répertoire cible pour l'image de l'Agent Dr.Web ne contient pas l'installateur de l'Agent Dr.Web pour les réseaux avec **Active Directory** (`<nom_du_package>.msi`).



Après le déploiement du package administrateur, le répertoire `<répertoire_cible>\Program Files\DrWeb` ne doit contenir que le fichier `README.txt`.

1. Afin de lancer l'installateur en mode graphique, exécutez la commande suivante :

```
msiexec /a <chemin_vers_l'installateur>\<nom_du_package>.msi
```

2. La fenêtre de l'assistant **InstallShield Wizard** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **Suivant**.



L'installateur de l'Agent Dr.Web utilise la langue spécifiée dans les options linguistiques de l'ordinateur.

3. Dans la nouvelle fenêtre, spécifiez le nom DNS ou l'adresse IP du Serveur Dr.Web (voir le document **Annexes**, [Annexe D. Spécification de l'adresse réseau](#)). Spécifiez également l'emplacement du certificat du Serveur Dr.Web (`drwcsd-certificate.pem`). Cliquez ensuite sur le bouton **Suivant**.



4. Dans la fenêtre suivante, spécifiez le répertoire réseau vers lequel l'image de l'Agent Dr.Web sera enregistré. Le chemin vers l'image doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale ; ce répertoire doit être accessible depuis les postes ciblés. Cliquez ensuite sur **Installer**.
5. Après la fin de l'installation, la fenêtre de configuration permettant de spécifier l'installation des packages sur les postes dans le réseau sera affichée de manière automatique.

Configuration de l'installation du package sur les postes sélectionnés

1. Dans le **Panneau de configuration** (ou dans le menu **Démarrer** sous Windows Server 2003/2008/2012/2012R2, dans le menu **Démarrer** → **Tous les programmes** sous Windows Server 2000) sélectionnez **Administration** → **Active Directory — utilisateurs et ordinateurs** (en mode graphique de l'installation de l'Agent Dr.Web cette fenêtre s'affiche de manière automatique).
2. Dans le domaine contenant les ordinateurs sur lesquels les Agents Dr.Web seront installés, créez une nouvelle **Unité** (sous Windows Server 2000 — **Unité d'organisation**) nommée par exemple **ESS**. Pour ce faire, dans le menu contextuel, sélectionnez **Créer** → **Unité**. Dans la fenêtre qui s'affiche, entrez le nom de cette nouvelle unité et cliquez sur **OK**. Ajoutez à cette unité les ordinateurs sur lesquels vous souhaitez installer l'Agent Dr.Web.
3. Ouvrez la fenêtre d'édition des politiques de groupe. Pour cela, procédez comme suit :
 - a) sous Windows Server 2000/2003 : dans le menu contextuel de l'unité créée **ESS**, sélectionnez l'élément **Propriétés**. Dans la fenêtre qui apparaît, passez à l'onglet **Politique de groupe**.
 - b) sous Windows 2008/2012/2012R2 : cliquez sur **Démarrer** → **Administration** → **Gestion de la politique de groupe**.
4. Spécifiez une politique de groupe pour l'unité créée. Pour cela, procédez comme suit :
 - a) Sous Windows 2000/2003 : double cliquez sur le bouton **Ajouter** et créez un élément de la liste avec le nom de la politique **ESS**. Double cliquez sur cet élément.
 - b) Sous Windows 2008/2012/2012R2 : dans le menu contextuel de l'unité créée **ESS**, sélectionnez l'élément **Créer un objet GPO dans ce domaine, et le lier**. Dans la fenêtre qui apparaît, spécifiez le nom du nouvel objet de la politique de groupe et cliquez ensuite sur **OK**. Dans le menu contextuel de la nouvelle politique, sélectionnez l'élément **Modifier**.
5. La fenêtre **Éditeur d'objets de stratégie de groupe** sera ouverte, spécifiez les paramètres relatifs à la politique de groupe créée à l'étape 4. Pour ce faire, procédez comme suit :
 - a) Sous Windows 2000/2003 : depuis l'arborescence sélectionnez l'élément **Configuration ordinateur** → **Paramètres du logiciel** → **Installations des logiciels**.
 - b) Sous Windows 2008/2012/2012R2 : depuis l'arborescence sélectionnez l'élément **Configuration ordinateur** → **Stratégies** → **Paramètres du logiciel** → **Installations des logiciels**.
6. Dans le menu contextuel de l'élément **Installations des logiciels**, sélectionnez l'élément **Créer** → **Package**.



7. Spécifiez le package d'installation de l'Agent Dr.Web. Pour cela, spécifiez l'adresse de la ressource réseau partagée (image de l'Agent Dr.Web créé lors de l'installation en mode administrateur). Le chemin vers le répertoire contenant le package doit être spécifié au format adresse réseau même si le répertoire se trouve sur la machine locale.
8. La fenêtre **Déploiement du logiciel** s'affiche. Sélectionnez l'option **Attribués**. Cliquez sur **OK**.
9. L'élément **Dr.Web Agent** sera présent dans la fenêtre de l'éditeur d'objets de stratégie de groupe. Depuis le menu contextuel de cet élément sélectionnez **Propriétés**.
10. Dans la fenêtre de propriétés du package qui apparaît, passez à l'onglet **Déploiement**. Cliquez sur le bouton **Avancé**.
11. La fenêtre **Options de déploiement avancées** sera ouverte.
 - Cochez la case **Ignorer la langue lors du déploiement**.
 - Si vous planifiez l'installation de l'Agent Dr.Web avec un package msi configurable sur les OS 64 bits, activez la case **Rendre cette application 32 bits disponible sur les ordinateurs x64**.
12. Double cliquez sur **OK**.
13. L'Agent Dr.Web sera installé sur les postes sélectionnés au prochain enregistrement dans le domaine.

Réalisation des politiques en fonction des installations antérieures de l'Agent Dr.Web

Lors de la spécification des politiques Active Directory relatives à l'installation de l'Agent Dr.Web, il est nécessaire de prendre en compte le cas où l'Agent Dr.Web pouvait déjà être installé sur le poste. Les trois options sont possibles :

1. L'Agent Dr.Web n'est pas présent sur le poste.

Après l'application des stratégies, l'Agent sera installé selon la règle générale.

2. L'Agent Dr.Web est déjà installé sur le poste mais sans utiliser le service Active Directory.

Après l'application de la politique Active Directory, l'Agent Dr.Web installé reste sur le poste.



Dans ce cas-là, l'Agent Dr.Web est installé sur le poste, mais le service Active Directory considère l'Agent Dr.Web comme non installé. C'est pourquoi, à chaque démarrage du poste, il y aura des tentatives inutiles d'installer l'Agent Dr.Web via le service Active Directory.

Afin d'installer l'Agent Dr.Web via Active Directory, il est nécessaire de supprimer l'Agent Dr.Web de manière manuelle (ou avec le Centre de gestion) et de redéterminer les politiques Active Directory pour le poste en question.



3. L'Agent Dr.Web est déjà installé sur le poste avec l'utilisation du service Active Directory.

Il est impossible de redéterminer la stratégie pour le poste avec l'Agent Dr.Web installé via le service Active Directory.

Ainsi, la détermination des stratégies ne va pas influencer le statut du logiciel antivirus sur le poste.

5.3. Installation du Serveur de scan Dr.Web



Le Serveur de scan peut être installé uniquement sous les OS de la famille Linux et FreeBSD.

Le serveur de scan et les machines virtuelles avec l'Agent Dr.Web installé qu'il dessert doivent se placer au sein d'un seul hyperviseur.

1. Téléchargez le package d'installation du Serveur de scan depuis la [page d'installation](#) sur le poste que vous voulez désigner comme Serveur de scan.
2. Téléchargez le certificat du Serveur Dr.Web auquel le Serveur de scan va se connecter. Pour ce faire, sélectionnez l'élément **Clés de chiffrement** dans la section **Administration**. Cochez la case contre l'objet **Certificat** et cliquez sur **Exporter**. Téléchargez le certificat sur le poste que vous voulez désigner comme Serveur de scan.



Vous pouvez télécharger le certificat sur la même page d'installation. Le certificat se trouve dans le même répertoire que le package d'installation du Serveur de scan.

3. Allez dans le répertoire duquel le fichier d'installation a été téléchargé et autorisez son exécution :

```
# chmod +x <nom_du_fichier> .run
```

4. Ensuite, lancez la procédure d'installation :

```
# ./<nom_du_fichier> .run
```

5. Acceptez les termes du Contrat de licence.
6. Une fois l'installation terminée, connectez le poste que vous voulez désigner comme Serveur de scan au Serveur Dr.Web en exécutant la commande :

```
# drweb-ctl esconnect <adresse du Serveur Dr.Web> --Certificate <chemin d'accès au fichier de certificat>
```




Il est recommandé d'utiliser le nom de serveur [au format FQDN](#) en tant qu'adresse du Serveur Dr.Web.

Après l'exécution de cette commande, la connexion doit être autorisée automatiquement ou par l'administrateur du réseau antivirus en fonction des configurations du Serveur Dr.Web.



Vous pouvez vous connecter au Serveur Dr.Web d'une autre façon : [créez un compte du poste](#) que vous voulez désigner comme Serveur de scan. Après cela, vous recevrez un login (ID du poste) et un mot de passe pour la connexion. Ensuite, exécutez la commande :

```
# drweb-ctl esconnect <adresse du Serveur Dr.Web> --login <ID du poste> --password <mot de passe> --Certificate <chemin d'accès au fichier de certificat>
```

7. En cas de connexion réussie, le poste sera marqué dans l'arborescence du réseau antivirus par l'icône  qui indique que le Serveur de scan est actif et prêt à s'exécuter.



L'installation de l'Agent Dr.Web sur le poste remplissant les fonctions du Serveur de scan n'est pas requise.

8. Assurez-vous que le Serveur de scan écoute les ports 7090 et 18008 en exécutant la commande suivante :

```
# netstat -l
```

La sortie de cette commande doit comporter les lignes suivantes :

```
tcp 0 0 0.0.0.0:7090 0.0.0.0:* LISTEN
udp 0 0 0.0.0.0:18008 0.0.0.0:*
```



Vous trouverez les informations détaillées sur la configuration du Serveur de scan et la connexion de postes dans le **Manuel Administrateur Dr.Web Enterprise Security Suite**, dans la section [Connexion de postes au Serveur de scan.](#)

5.4. Installation de NAP Validator

Dr.Web NAP Validator sert à vérifier le fonctionnement de l'antivirus tournant sur les postes protégés.

Ce composant peut être installé sur le poste ayant le serveur NAP configuré.

Pour installer NAP Validator

1. Lancez le fichier d'installation. Dans la fenêtre qui apparaît, sélectionnez la langue à utiliser lors de l'installation. Sélectionnez **Français** et cliquez sur **Suivant**.
2. La fenêtre de l'assistant **InstallShield Wizard** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **Suivant**.
3. La fenêtre affichant le texte du Contrat de licence va s'ouvrir. Après avoir pris connaissance des termes du Contrat, indiquez **J'accepte les termes du Contrat de licence** et cliquez sur **Suivant**.



4. Dans la fenêtre qui s'affiche, dans les champs **Adresse** et **Port** entrez l'adresse IP et le port de Serveur Dr.Web. Cliquez sur **Suivant**.
5. Cliquez sur le bouton **Installer**. Les actions suivantes du programme d'installation ne nécessitent aucune intervention de l'utilisateur.
6. Après la fin de l'installation, cliquez sur le bouton **Terminer**.

Après l'installation de Dr.Web NAP Validator, il est nécessaire d'ajouter le Serveur Dr.Web dans le groupe de serveurs NAP de confiance. Pour cela, procédez comme suit :

1. Ouvrez le composant de la configuration du serveur NAP (avec la commande `nps.msc`).
2. Dans la rubrique **Groupe de Serveurs de remédiation** cliquez sur le bouton **Ajouter**.
3. Dans la boîte de dialogue qui s'ouvre, spécifiez le nom pour le serveur de remédiation et l'adresse IP du Serveur Dr.Web.
4. Pour appliquer les modifications apportées, cliquez sur **OK**.

5.5. Installation du Serveur proxy Dr.Web

Le réseau antivirus peut comprendre un ou plusieurs Serveurs proxy Dr.Web.

Pour sélectionner l'ordinateur sur lequel sera installé le Serveur proxy Dr.Web, il faut prendre en compte que le critère principal est l'accessibilité du Serveur proxy Dr.Web depuis tous les réseaux/fragments de réseau entre lesquels il doit rediriger des informations.



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

Vous pouvez installer le Serveur proxy Dr.Web sous Windows par l'un des moyens suivants :

- [Automatiquement lors de l'installation de l'Agent Dr.Web pour Windows](#)

L'installation s'effectue depuis le package d'installation personnel de l'Agent Dr.Web pendant la création duquel les paramètres pour l'installation du Serveur proxy Dr.Web lié ont été spécifiés. Dans ce cas, l'installation du Serveur proxy Dr.Web se fait automatiquement en tâche de fond.

- [Automatiquement sur le poste avec l'Agent Dr.Web pour Windows installé](#)

Dans le Centre de gestion du poste sélectionné, configurez la création du Serveur proxy Dr.Web lié. Le Serveur proxy Dr.Web sera installé sur le poste automatiquement en tâche de fond.

- [Manuellement avec l'installateur graphique](#)

L'administrateur effectue l'installation manuellement sur tout poste approprié du réseau. Aucun autre composant du réseau antivirus ne peut être installé sur ce poste.



L'installation du Serveur proxy Dr.Web sous l'OS de la famille UNIX ne se fait que [manuellement à l'aide de l'installateur](#).

5.5.1. Création d'un compte du Serveur proxy Dr.Web



L'administrateur doit créer les comptes du Serveur proxy Dr.Web sur tous les Serveurs Dr.Web auxquels le Serveur proxy Dr.Web se connectera (vers lesquels le trafic sera redirigé).

Pour créer un compte du Serveur proxy Dr.Web à l'aide du Centre de gestion de la sécurité Dr.Web

1. Spécifiez les paramètres pour le groupe parent dans lequel vous allez créer le Serveur proxy Dr.Web. La procédure de configuration des paramètres est décrite dans le **Manuel Administrateur**, dans la rubrique [Configuration distante du Serveur proxy](#). Dans ce cas, les paramètres spécifiés seront hérités par le Serveur proxy Dr.Web lors de la connexion. Vous pouvez également spécifier ces paramètres après la création du compte du Serveur proxy Dr.Web (tant pour le groupe parent en cas d'héritage que personnellement pour le Serveur proxy Dr.Web) mais avant la connexion du Serveur proxy Dr.Web au compte.




Si les paramètres n'ont pas été spécifiés avant la connexion du Serveur proxy Dr.Web, le fichier de configuration ne sera pas téléchargé. Le Serveur proxy Dr.Web utilisera les paramètres actuels jusqu'à ce que les paramètres soient spécifiés sur le Serveur Dr.Web connecté, à condition qu'il soit autorisé à gérer la configuration.

2. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
3. Les actions nécessaires pour la création du Serveur proxy Dr.Web dépendront du fait que vous vouliez installer le Serveur proxy Dr.Web sur le poste existant avec l'Agent Dr.Web ou installer le Serveur proxy Dr.Web séparément :

N°	Actions	Installer avec l'Agent Dr.Web	Installer séparément
a)	<ol style="list-style-type: none">1. Dans l'arborescence du réseau antivirus, sélectionnez le poste pour l'installation du Serveur proxy Dr.Web lié.2. Dans le panneau de propriétés du poste sélectionné, ouvrez la section Serveur proxy.	+	-
b)	<ol style="list-style-type: none">1. Dans l'arborescence du réseau antivirus, sélectionnez le poste pour l'installation du Serveur proxy Dr.Web lié.2. Dans la barre d'outils, sélectionnez l'option + Ajouter un objet de réseau → + Créer un Serveur proxy.	+	+
c)	<ol style="list-style-type: none">1. Assurez-vous qu'aucun poste n'est sélectionné dans l'arborescence du réseau antivirus.	+	+



N°	Actions	Installer avec l'Agent Dr.Web	Installer séparément
2.	Dans la barre d'outils, sélectionnez l'option + Ajouter un objet de réseau →  + Créer un Serveur proxy.		



Si vous créez un compte du Serveur proxy Dr.Web pour l'installation sur les postes avec l'Agent Dr.Web, l'installation du Serveur proxy Dr.Web s'effectuera automatiquement via l'Agent en tâche de fond, juste après la création du compte du Serveur proxy (voir aussi [Installation du Serveur proxy Dr.Web lors de l'installation de l'Agent Dr.Web pour Windows](#)).

Si vous créez un compte du Serveur proxy Dr.Web pour l'installation particulière (sans liaison à l'Agent Dr.Web), l'administrateur devra installer le Serveur proxy Dr.Web manuellement depuis le package d'installation fourni avec la distribution du Serveur Dr.Web.

- L'identificateur unique du compte créé est généré automatiquement dans le champ **Identificateur**. Si nécessaire, vous pouvez le modifier.
- Dans le champ **Nom**, spécifiez le nom du Serveur proxy Dr.Web qui sera affiché dans l'arborescence du réseau antivirus.




Le nom spécifié lors de la configuration sera automatiquement remplacé par le nom de l'ordinateur après la connexion du Serveur proxy Dr.Web au Serveur Dr.Web.

- Dans les champs **Mot de passe** et **Confirmez le mot de passe**, entrez le mot de passe pour que le Serveur proxy puisse accéder au Serveur Dr.Web. Si le mot de passe n'est pas spécifié, il sera généré automatiquement.




L'identificateur et le mot de passe du Serveur proxy Dr.Web sont utilisés en unique exemplaire. Sur tous les Serveurs Dr.Web auxquels le Serveur proxy Dr.Web se connecte, vous devez créer des comptes du Serveur proxy Dr.Web avec les mêmes identifiants (voir [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#)).

Après la création du compte du Serveur proxy Dr.Web, l'édition de l'identificateur sera impossible.

- Pour les étapes 3.b) et 3.c) dans le champ **Poste**, spécifiez un poste existant avec l'Agent Dr.Web installé auquel ce Serveur proxy Dr.Web sera lié.
Pour l'étape 3.b), l'identificateur du poste sélectionné sera automatiquement ajouté dans le champ **Poste**.
Pour l'étape 3.c), le champ **Poste** reste vide.
 - Pour spécifier un poste sur lequel le Serveur proxy Dr.Web sera installé, cliquez sur  et, dans la fenêtre qui s'affiche, sélectionnez un poste existant dans l'arborescence du réseau antivirus.



- Laissez le champ **Poste** vide pour ne pas lier le Serveur proxy Dr.Web à un poste et connecter le Serveur proxy Dr.Web installé manuellement. Si le champ **Poste** est déjà rempli, cliquez sur **X** pour supprimer le poste lié.
8. La section **Appartenance** contient le groupe dont le Serveur proxy Dr.Web créé fera partie. Pour modifier le groupe, cochez la case contre le groupe nécessaire dans la liste affichée. Chaque Serveur proxy peut appartenir à un seul groupe. Il est possible de sélectionner un groupe prédéfini **Proxies** ou ses sous-groupes.
 9. Cliquez sur **Enregistrer**. La fenêtre annonçant la création réussie du compte du Serveur proxy Dr.Web va s'afficher. Cette fenêtre contiendra également le mot de passe d'accès au Serveur Dr.Web. Pour afficher le mot de passe, cliquez .



L'administrateur a besoin de l'identificateur et du mot de passe du compte du Serveur proxy Dr.Web créé via le Centre de gestion pour la connexion du Serveur proxy Dr.Web au Serveur Dr.Web :

- [Lors de l'installation du Serveur proxy via l'installateur graphique.](#)
- [Manuellement après l'installation du Serveur proxy \(uniquement pour les OS de la famille UNIX\).](#)

5.5.2. Installation du Serveur proxy Dr.Web lors de l'installation de l'Agent Dr.Web pour Windows

Pour installer le Serveur proxy Dr.Web avec l'Agent Dr.Web pour Windows

1. Spécifiez les paramètres du Serveur proxy Dr.Web dans le Centre de gestion comme cela est décrit dans le **Manuel Administrateur**, le p. [Configuration distante du Serveur proxy](#). Les paramètres doivent être spécifiés pour le groupe dans lequel vous allez créer le Serveur proxy. Dans ce cas, les paramètres spécifiés seront hérités par le Serveur proxy au moment de la création. Vous pouvez également spécifier ces paramètres après la création du Serveur proxy (tant pour le groupe en cas d'héritage que personnellement pour le Serveur proxy Dr.Web) mais avant la connexion du Serveur proxy Dr.Web au compte créé.



Si les paramètres n'ont pas été spécifiés avant la connexion du Serveur proxy Dr.Web, les paramètres transmis au Serveur proxy Dr.Web par l'installateur seront utilisés. Ces paramètres impliquent seulement la connexion au Serveur Dr.Web depuis lequel l'installation a été effectuée.

2. Créez le compte du poste à l'aide du Centre de gestion comme cela est décrit dans la rubrique [Installation de l'Agent Dr.Web avec le package d'installation personnel](#). Lors de la création du compte, cochez la case **Créer un Serveur proxy lié** et spécifiez les paramètres. Notamment, indiquez le groupe pour le placement du Serveur proxy Dr.Web pour lequel vous avez spécifié les paramètres à l'étape 1.



Vous pouvez modifier l'identificateur du Serveur proxy Dr.Web uniquement lors de la création du compte.

3. Sur le poste, lancez l'installation de l'Agent Dr.Web depuis le package d'installation personnel créé à l'étape 2.
4. Après l'installation, l'Agent Dr.Web télécharge automatiquement l'installateur du Serveur proxy Dr.Web depuis le Serveur Dr.Web et lance l'installateur en tâche de fond sur le même poste. Le certificat et l'adresse du Serveur Dr.Web, ainsi que les identifiants utilisés pour la connexion au Serveur Dr.Web seront automatiquement inscrits dans les fichiers de configuration du Serveur proxy Dr.Web. Seul le Serveur Dr.Web depuis lequel l'installation a été effectuée est indiqué dans les paramètres du Serveur proxy Dr.Web pour la redirection du trafic.
5. Après l'installation, le Serveur proxy Dr.Web se connectera au Serveur Dr.Web depuis lequel l'installation a été effectuée pour la réception du fichier de configuration valide. Si les paramètres n'ont pas été spécifiés à l'étape 1, le fichier de configuration ne sera pas téléchargé. La configuration spécifiée par l'installateur sera utilisée jusqu'à ce que la configuration sur le Serveur Dr.Web connecté soit spécifiée.
6. L'Agent Dr.Web se connectera au Serveur uniquement via le Serveur proxy Dr.Web installé. L'utilisation du Serveur proxy Dr.Web sera transparente pour l'utilisateur.

5.5.3. Installation du Serveur proxy Dr.Web avec l'installateur



Les droits d'administrateur du poste sont requis pour installer le Serveur proxy Dr.Web.

Installation du Serveur proxy Dr.Web sous Windows

1. Créez un compte du Serveur proxy Dr.Web à l'aide du Centre de gestion de la sécurité Dr.Web, comme cela est décrit dans la rubrique [Création d'un compte du Serveur proxy Dr.Web](#).
2. Téléchargez l'installateur du Serveur proxy Dr.Web depuis la [page d'installation](#).
3. Copiez le certificat du Serveur Dr.Web auquel le Serveur proxy se connectera (voir [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#)) et l'installateur du Serveur proxy Dr.Web sur le poste sur lequel vous voulez effectuer l'installation.
4. Lancez l'installateur du Serveur proxy Dr.Web. La fenêtre de l'assistant **Installation du Serveur proxy Dr.Web** apparaît et vous informe sur le produit en cours d'installation. Cliquez sur le bouton **Suivant**.
5. Dans la fenêtre de paramètres généraux du Serveur proxy Dr.Web, spécifiez les paramètres essentiels suivants dans la section **Paramètres d'écoute du réseau** :
 - Dans le champ **Adresse d'écoute**, spécifiez l'adresse IP « écoutée » par le Serveur proxy Dr.Web. Par défaut toutes les interfaces sont « écoutées ».



Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, dans la rubrique [Annexe D. Spécification de l'adresse réseau](#).

- Dans le champ **Port**, spécifiez le numéro du port qui sera « écouté » par le Serveur proxy Dr.Web. Par défaut c'est le port 2193.
- Cochez la case **Activer la détection** pour activer le mode d'imitation du Serveur Dr.Web. Ce mode permet au clients de détecter le Serveur proxy Dr.Web en tant que Serveur Dr.Web lors de sa recherche par les requêtes broadcast.
- Cochez la case **Activer la multidiffusion** pour que le Serveur proxy Dr.Web réponde aux requêtes broadcast adressées au Serveur Dr.Web.
 - Dans le champ **Adresse du groupe de multidiffusion**, entrez l'adresse IP du groupe de multidiffusion dont le Serveur proxy Dr.Web fera partie. L'interface spécifiée sera écoutée par le Serveur proxy Dr.Web afin d'assurer l'interaction avec les clients lors de la recherche des Serveurs Dr.Web actifs. Si vous laissez le champ vide, le Serveur proxy Dr.Web ne sera inclus dans aucun groupe de multidiffusion. Par défaut, le Serveur Dr.Web appartient au groupe de multidiffusion 231.0.0.1.

Dans la section **Paramètres de la connexion client** :

- Dans la liste déroulante **Mode de compression**, sélectionnez le mode de compression du trafic pour les canaux entre le Serveur proxy Dr.Web et les clients servis : les Agents Dr.Web et les installateurs des Agents Dr.Web. Dans la liste déroulante **Niveau**, spécifiez le niveau de compression (de 1 à 9).
- Dans la liste déroulante **Mode de chiffrement**, sélectionnez le mode de chiffrement du trafic pour les canaux entre le Serveur proxy Dr.Web et les clients servis : les Agents Dr.Web et les installateurs des Agents Dr.Web.

Pour plus d'infos sur le chiffrement et la compression, consultez la section [Chiffrement et compression du trafic](#).

Cliquez sur le bouton **Suivant**.

6. Spécifiez les paramètres de redirection des connexions :


- Saisissez l'adresse du Serveur Dr.Web vers lequel les connexions établies par le Serveur proxy Dr.Web seront redirigées et cliquez sur . Après l'installation le Serveur proxy Dr.Web se connectera à ce Serveur proxy Dr.Web pour obtenir la configuration. Le certificat de ce Serveur Dr.Web a été copié sur le poste à l'étape 3.




Les adresses sont spécifiées au format d'adresse réseau décrit dans le document **Annexes**, dans la rubrique [Annexe D. Spécification de l'adresse réseau](#).

- Dans la liste déroulante **Chiffrement**, sélectionnez le mode de chiffrement du trafic pour les canaux de communication entre le Serveur proxy Dr.Web et le Serveur Dr.Web spécifié.
- Dans la liste déroulante **Compression** sélectionnez le mode de compression du trafic pour les canaux de communication entre le Serveur proxy Dr.Web et le Serveur Dr.Web spécifié. Dans la liste déroulante **Niveau**, sélectionnez le niveau de compression (de 1 à 9).



Pour ajouter encore un Serveur Dr.Web à la liste de redirection du trafic, saisissez son adresse dans le champ, cliquez sur le bouton  et spécifiez les paramètres de chiffrement et de compression.

Pour supprimer de la liste de redirection du trafic la dernière adresse ajoutée du Serveur Dr.Web, cliquez sur le bouton .



Après la fin de l'installation le Serveur proxy Dr.Web se connectera au premier Serveur Dr.Web spécifié dans cette section pour obtenir les paramètres.

Si la configuration du Serveur proxy Dr.Web est spécifiée sur le Serveur Dr.Web, tous les paramètres spécifiés dans l'installateur seront réécrits pour la nouvelle configuration obtenue du Serveur Dr.Web.

Après avoir édité les paramètres de redirection, cliquez sur **Suivant**.

7. La fenêtre de configuration de la connexion au Serveur Dr.Web s'ouvrira pour la gestion à distance.

La connexion se fait au premier Serveur Dr.Web spécifié à l'étape 6 pour la redirection du trafic.

- Dans le champ **Certificat du Serveur**, spécifiez le fichier du certificat copié sur le poste à l'étape 3. Pour sélectionner le fichier, cliquez sur **Parcourir**.
- Dans les champs **Identificateur** et **Mot de passe**, spécifiez les identifiants du compte créé sur le Serveur Dr.Web à l'étape 1.

Cliquez sur **Suivant**.

8. Dans la fenêtre **Paramètres de mise en cache** spécifiez les paramètres de mise en cache du Serveur proxy Dr.Web :

Cochez la case **Activer la mise en cache** pour mettre en cache les données transmises par le Serveur proxy Dr.Web et spécifiez les paramètres suivants :

- Dans le champ **Périodicité de suppression des révisions (minutes)**, spécifiez la périodicité de suppression des anciennes révisions du cache au cas où leur nombre dépasserait le nombre maximum autorisé des révisions stockés. La valeur est spécifiée en minutes. Par défaut c'est 60 minutes.
 - Dans le champ **Nombre des révisions à sauvegarder**, spécifiez le nombre maximal des révisions de chaque produit qui seront stockés dans le cache après le nettoyage. Par défaut, les 3 dernières révisions sont sauvegardées, les révisions plus anciennes sont supprimées.
- Dans le champ **Période de déchargement des fichiers non utilisés (minutes)**, spécifiez l'intervalle de temps en minutes entre les déchargements des fichiers non utilisés de la mémoire vive. La valeur spécifiée par défaut est de 10 minutes.

Après avoir spécifié les paramètres de mise en cache, cliquez sur **Suivant**.

9. La fenêtre informant sur la disponibilité de l'installation du Serveur proxy Dr.Web va s'ouvrir.



S'il faut modifier les paramètres supplémentaires de l'installation, notamment le répertoire d'installation du Serveur proxy Dr.Web et le chemin d'emplacement des fichiers utilisés par le Serveur proxy Dr.Web, cliquez sur **Paramètres avancés**.

Pour commencer l'installation du Serveur proxy Dr.Web, cliquez sur le bouton **Installer**.

10. Une fois l'installation terminée, cliquez sur le bouton **Quitter**.

11. Après l'installation, le Serveur proxy Dr.Web se connectera au Serveur Dr.Web spécifié à l'étape 6 pour la réception du fichier de configuration valide. Si les paramètres n'ont pas été spécifiés, le fichier de configuration ne sera pas téléchargé. La configuration spécifiée par l'installateur sera utilisée jusqu'à ce que la configuration sur le Serveur Dr.Web connecté soit spécifié.

Installation du Serveur proxy Dr.Web sous les OS de la famille UNIX

1. Téléchargez l'installateur du Serveur proxy Dr.Web depuis la [page d'installation](#).

2. Lancez l'installateur du Serveur proxy Dr.Web à l'aide de la commande suivante :

```
./<fichier_de_distribution>.tar.gz.run
```

3. Pour continuer l'installation, veuillez accepter le contrat de licence.

4. Indiquez le chemin d'accès au certificat du Serveur Dr.Web. Vous pouvez également ajouter le certificat après l'installation du Serveur proxy Dr.Web (voir [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#)).

5. Si nécessaire, vous pouvez utiliser les fichiers de configuration de l'installation précédente du Serveur proxy Dr.Web :

- Pour utiliser la copie de sauvegarde enregistrée par défaut dans le dossier `/var/tmp/drwcsd-proxy`, cliquez sur ENTRER.
- Pour utiliser une copie de sauvegarde se trouvant dans un autre dossier, indiquez le chemin d'accès manuellement.
- Vous pouvez également installer le Serveur proxy Dr.Web avec les paramètres par défaut sans utiliser la copie de sauvegarde de la configuration de l'installation précédente. Pour ce faire, cliquez sur 0.

6. Après l'installation du Serveur proxy Dr.Web, vous pouvez éditer les fichiers de configuration correspondants si cela est nécessaire (voir [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#)).

Démarrage et arrêt

Au cours de l'installation du logiciel sous l'OS **FreeBSD** le script `rc /usr/local/etc/rc.d/dwcp_proxy` est créé. Utilisez les commandes :

- `/usr/local/etc/rc.d/dwcp_proxy stop` : pour arrêter manuellement le Serveur proxy Dr.Web ;



- `/usr/local/etc/rc.d/dwcp_proxy start` : pour démarrer manuellement le Serveur proxy Dr.Web.

Lors de l'installation du logiciel sous **Linux**, le script `init` pour le lancement et l'arrêt du Serveur proxy Dr.Web `/etc/init.d/dwcp_proxy` sera créé.

5.5.4. Connexion du Serveur proxy Dr.Web au Serveur Dr.Web

A partir de la version 11, il existe la possibilité de connexion du Serveur proxy Dr.Web au Serveur Dr.Web pour la gestion distante des paramètres et le support du chiffrement du trafic.

Paramètres de connexion

La connexion du Serveur proxy Dr.Web au Serveur Dr.Web demande :

- **Certificat du Serveur Dr.Web** `drwcsd-certificate.pem`.

Il faut que les certificats de tous les Serveurs Dr.Web auxquels le Serveur proxy Dr.Web se connecte et vers lesquels le trafic client est redirigé soient disponibles.

- Le certificat du Serveur Dr.Web est requis pour la connexion au Serveur Dr.Web afin de gérer à distance les paramètres et chiffrer le trafic entre le Serveur Dr.Web et le Serveur proxy Dr.Web.
- Le certificat du Serveur proxy Dr.Web signé par le certificat et la clé privée du Serveur Dr.Web (la procédure se fait automatiquement sur le Serveur Dr.Web après la connexion et elle ne nécessite pas l'intervention de l'administrateur) est requis pour la connexion des Agents Dr.Web et le support du chiffrement entre les Agents Dr.Web et le Serveur proxy Dr.Web.

Tous les certificats des Serveurs Dr.Web sont stockés sur le Serveur proxy Dr.Web dans le fichier de configuration `drwcsd-proxy-trusted.list` au format suivant (les entrées des certificats sont séparées par une ou plusieurs lignes vides) :

```
[<certificat_1>

[<certificat_2>

[<certificat_3>

...
```

- **Adresse du Serveur Dr.Web.**

Le Serveur proxy Dr.Web se connecte à tous les Serveurs Dr.Web qui sont indiqués dans son fichier de configuration pour la redirection du trafic client. Pourtant, la réception des



paramètres est autorisée seulement depuis un ensemble particulier des Serveurs Dr.Web qui sont marqués comme gérants. Si plusieurs Serveurs Dr.Web sont marqués comme gérants, la connexion se fait à tous les Serveurs Dr.Web à tour de rôle jusqu'à l'obtention d'une configuration valide (non vide).

• **Identificateur et mot de passe pour l'accès au Serveur Dr.Web.**

Les identifiants sont disponibles après la création du compte du Serveur proxy Dr.Web via le Centre de gestion (voir [Création d'un compte du Serveur proxy Dr.Web](#)).



L'identificateur et le mot de passe du Serveur proxy Dr.Web sont utilisés en unique exemplaire. Sur tous les Serveurs Dr.Web auxquels le Serveur proxy Dr.Web se connecte, vous devez créer des comptes du Serveur proxy Dr.Web avec les mêmes identifiants.

Les identifiants sont sauvegardés sur le Serveur proxy Dr.Web, dans le fichier de configuration `drwcsd-proxy.auth` au format suivant :

```
[ <ID_du_Serveur_proxy> ]  
[ <Mot_de_passe_du_Serveur_proxy> ]
```

Connexion du Serveur proxy Dr.Web au Serveur Dr.Web



Pour pouvoir connecter le Serveur proxy Dr.Web, il faut activer le protocole nécessaire du côté du Serveur Dr.Web. Pour ce faire, dans le Centre de gestion, dans la section **Administration** → **Configuration du Serveur Dr.Web** → **Modules**, cochez la case **Protocole du Serveur proxy Dr.Web**, enregistrez les paramètres et redémarrez le Serveur Dr.Web.

Connexion automatique lors de l'installation sous l'OS Windows :

- Si le Serveur proxy Dr.Web a été installé [durant l'installation de l'Agent Dr.Web](#) ou [sur un poste avec l'Agent Dr.Web](#) installé, la connexion au Serveur Dr.Web se fait automatiquement.
- Si le Serveur proxy Dr.Web a été installé via [l'installateur graphique sous Windows](#), la connexion au Serveur Dr.Web se fait automatiquement avec les paramètres de connexion indiqués par l'administrateur dans les paramètres de l'installateur.

Après l'installation du Serveur proxy Dr.Web, les fichiers de connexion au Serveur Dr.Web se trouvent par défaut dans le répertoire : `C:\ProgramData\Doctor Web\drwcs\etc.`

Connexion manuelle sous l'OS de la famille UNIX :

1. Installez le Serveur proxy Dr.Web pour les OS de la famille UNIX conformément à la procédure décrite dans la rubrique [Installation du Serveur proxy Dr.Web avec l'installateur](#).



2. Créez un compte du Serveur proxy Dr.Web à l'aide du Centre de gestion de la sécurité Dr.Web, comme cela est décrit dans la rubrique [Création d'un compte du Serveur proxy Dr.Web](#).
3. Copiez le certificat du Serveur Dr.Web sur l'ordinateur sur lequel le Serveur proxy Dr.Web est installé.
4. Dans le fichier de configuration `drwcsd-proxy-trusted.list`, indiquez le certificat, copié sur l'ordinateur à l'étape 3 : copiez le contenu du fichier de certificat et insérez-le dans le fichier de configuration conformément au format décrit [ci-dessus](#).
5. Dans le fichier de configuration `drwcsd-proxy.auth`, spécifiez les paramètres de connexion au Serveur Dr.Web pour le compte créé à l'étape 2 conformément au format décrit [ci-dessus](#).

Les fichiers `drwcsd-proxy-trusted.list` et `drwcsd-proxy.auth` doivent se trouver dans les répertoires suivants :

- sous Linux : `/var/opt/drwcs/etc`
- sous FreeBSD : `/var/drwcs/etc`

Pour les fichiers, il faut spécifier les droits suivants :

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs
drwcsd-proxy.auth 0600 drwcs:drwcs
```

Connexion rapide à l'aide de la ligne de commande

Cette option est particulièrement pertinente pour les OS de la famille UNIX, car elle élimine la nécessité d'éditer les fichiers de configuration manuellement. La commande unique peut être utilisée pour la connexion à un autre serveur, la réinitialisation des paramètres ou en cas des problèmes de la connexion déjà établie avec le serveur.

Utilisez les commandes suivantes :

- OS Windows :

```
drwcsd-proxy deploy <server-address> <server-certificate> <proxy-login>
<proxy-password>
```

- OS Linux :

```
/etc/init.d/dwcp_proxy deploy <server-address> <server-certificate> <proxy-
login> <proxy-password>
```

- OS FreeBSD :

```
/usr/local/etc/rc.d/dwcp_proxy deploy <server-address> <server-certificate>
<proxy-login> <proxy-password>
```




En cas de connexion réussie :

- Le nom d'utilisateur et le mot de passe sont enregistrés dans le fichier de configuration du Serveur proxy Dr.Web `drwcsd-proxy.auth`.
- Le certificat du Serveur Dr.Web est enregistré dans le fichier de configuration `drwcsd-proxy-trusted.list`.
- La nouvelle clé privée `drwcsd-proxy.pri` est générée.
- Le nouveau certificat est généré, signé sur le serveur et enregistré dans la liste des certificats signés du serveur proxy (`drwcsd-proxy-signed.list`).
- Le fichier de configuration est téléchargé du serveur et enregistré dans le fichier de configuration `drwcsd-proxy.conf`.

5.6. Codes d'erreur retournés lors de l'installation

Les codes d'erreur suivants seront retournés en cas d'erreurs lors de l'installation :

Code d'erreur	Description
0	L'installation est terminée avec succès
1	Format incorrect de la commande
2	Erreur inconnue
3	Droits insuffisants pour terminer l'opération (droits insuffisants pour écrire dans le registre, créer des fichiers ou exécuter des actions nécessaires pour l'installation)
4	L'Agent Dr.Web est déjà installé
5	L'installation est déjà lancée
7	L'installation est annulée
9	Le délai d'attente de la réponse du serveur est dépassé
11	Droits insuffisants pour supprimer l'application
12	La version du système d'exploitation est obsolète
13	Une application incompatible est détectée
14	Installation impossible. Veuillez redémarrer le système (le système attend un redémarrage avant une nouvelle tentative d'installation)
15	Architecture du système d'exploitation non prise en charge. Seuls x86 et x86_64 sont supportés



Code d'erreur	Description
16	Votre système d'exploitation ne supporte pas l'algorithme sha-2
50	Il est impossible de supprimer la version standalone en mode de tâche de fond

Pour savoir la cause de l'erreur, il vaut mieux regarder les enregistrements du journal. Les codes d'erreur listés ci-dessous sont communs, une erreur peut avoir des causes différentes.



Chapitre 6 : Suppression des composants Dr.Web Enterprise Security Suite

6.1. Suppression du Serveur Dr.Web

6.1.1. Suppression du Serveur Dr.Web sous Windows

Afin de désinstaller le logiciel du Serveur Dr.Web ou l'extension du Centre de gestion de la sécurité Dr.Web, lancez le package d'installation de la version correspondant à la version installée. L'installateur va détecter le produit installé de manière automatique et proposera de le supprimer. Pour désinstaller le logiciel, cliquez sur le bouton **Supprimer**.

La suppression du logiciel du Serveur Dr.Web peut également être effectuée avec les outils standard de l'OS Windows via l'élément suivant : **Panneau de configuration** → **Ajout/Suppression de programmes**.



En cas de suppression du Serveur Dr.Web, la copie de réserve des fichiers de configuration, des clés de chiffrement et des bases de données est effectuée uniquement si le paramètre Sauvegarder la copie de réserve des données critiques du **Serveur Dr.Web** est activé.

6.1.2. Suppression du Serveur Dr.Web sous les OS de la famille UNIX



Toutes les actions relatives à la suppression doivent être effectuées sous le nom de super-utilisateur (**root**).

Pour supprimer le Serveur Dr.Web en version 10 ou supérieure

OS du Serveur Dr.Web	Action
FreeBSD	Lancez le script : <code>/usr/local/etc/drweb.com/software/drweb-esuite.remove</code>
Linux	Lancez le script : <code>/etc/opt/drweb.com/software/drweb-esuite.remove</code>



Lors de la suppression du Serveur Dr.Web sous **FreeBSD** ou **Linux** les processus serveur seront arrêtés automatiquement, la base de données, les fichiers clés et les fichiers de configuration seront sauvegardés dans le répertoire par défaut — `/var/tmp/drwcs` (vous trouverez la liste de fichiers pour la copie de sauvegarde dans la rubrique [Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX](#)).

Pour annuler la copie de sauvegarde, il est nécessaire de spécifier la variable d'environnement `SKIP_BACKUP`. La variable peut prendre n'importe quelle valeur. Par exemple : `SKIP_BACKUP="x"`

Vous pouvez également ajouter la définition de la variable dans le fichier `common.conf`.

6.2. Suppression de l'Agent Dr.Web

La suppression de l'Agent Dr.Web depuis les postes protégés peut être réalisé par les moyens suivants :

- Pour les postes tournant sous Windows :
 - [Via le Centre de gestion](#).
 - [En mode local sur le poste](#).
 - [Via le service Active Directory](#), si l'Agent Dr.Web a été installé à l'aide de ce service.
- Pour les postes tournant sous l'OS Android, l'OS Linux, macOS — en mode local sur le poste.



La suppression de l'Agent Dr.Web sur les postes de travail tournant sous l'OS Android, l'OS Linux, macOS est décrite dans le **Manuel Utilisateur** pour le système d'exploitation correspondant.



6.2.1. Suppression de l'Agent Dr.Web pour Windows

Suppression à distance de l'Agent Dr.Web et du package antivirus



L'installation et la suppression du logiciel de l'Agent Dr.Web à distance ne peuvent être réalisées que dans le réseau local et nécessitent les droits d'administrateur dans ce réseau.



En cas de suppression de l'Agent et du package antivirus via le Centre de Contrôle, la Quarantaine ne sera pas supprimée du poste.

Pour supprimer l'antivirus du poste en mode distant (uniquement sous les OS de la famille Windows)

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui apparaît du répertoire du réseau antivirus, sélectionnez un groupe ou des postes antivirus particuliers.
3. Depuis la barre d'outils du répertoire du réseau antivirus cliquez sur **Général** → **Désinstaller l'Agent Dr.Web**.
4. Dans la fenêtre qui s'affiche **Désinstaller l'Agent Dr.Web**, vous pouvez configurer les paramètres de redémarrage automatique des postes sélectionnés après la suppression de l'Agent Dr.Web :
 - L'option **Tout de suite après la désinstallation** indique au poste de se redémarrer dans 5 minutes après la suppression de l'Agent Dr.Web.
 - L'option **À l'heure spécifiée** permet de préciser l'heure de redémarrage du postes par pas d'une heure.
 - L'option **Pendant la période spécifiée** permet de spécifier une plage horaire pendant laquelle un redémarrage sera effectué.

Quelle que soit l'option de redémarrage sélectionnée, l'utilisateur de poste recevra une notification de l'Agent Dr.Web sous forme d'une fenêtre pop-up.

Option de redémarrage	Notification de l'utilisateur
Non sélectionné	Le poste n'est pas redémarré après la suppression de l'Agent Dr.Web. Aucune notification.
Tout de suite après la désinstallation	La notification s'affiche 5 minutes avant le redémarrage et indique l'heure exacte de redémarrage du poste.
À l'heure spécifiée	<ul style="list-style-type: none">• Première notification La notification s'affiche tout de suite après la suppression de l'Agent Dr.Web et indique l'heure exacte de redémarrage.



Option de redémarrage	Notification de l'utilisateur
	<ul style="list-style-type: none">• Deuxième notification La notification s'affiche 5 minutes avant le redémarrage et indique l'heure exacte de redémarrage du poste.• S'il n'y a pas de liaison avec le poste à l'heure spécifiée 15 minutes après la restauration de la liaison, une notification s'affiche vous informant du redémarrage du poste dans 5 minutes avec l'indication de l'heure exacte.
Pendant la période spécifiée	<ul style="list-style-type: none">• Première notification La notification s'affiche tout de suite après la suppression de l'Agent Dr.Web et indique l'heure exacte de redémarrage du poste au cours de la période spécifiée.• Deuxième notification La notification s'affiche 5 minutes avant le redémarrage et indique l'heure exacte de redémarrage du poste.• S'il n'y a pas de liaison avec le poste pendant la période spécifiée 15 minutes après la restauration de la liaison, une notification s'affiche vous informant du redémarrage du poste le jour suivant avec l'indication de l'heure exacte.

5. Le logiciel de l'Agent Dr.Web et le package antivirus seront supprimés depuis les postes sélectionnés.



Si le processus de suppression est lancé alors qu'il n'y a pas de connexion entre le Serveur Dr.Web et le poste antivirus, la suppression du logiciel de l'Agent Dr.Web sur le poste sélectionné sera effectuée lorsque la connexion aura été rétablie.

Suppression locale de l'Agent Dr.Web et du package antivirus



La suppression locale de l'Agent Dr.Web et du package antivirus est possible à condition que cette option soit autorisée sur le Serveur Dr.Web dans la rubrique **Droits** (voir **Manuel Administrateur**, p. [Droits des utilisateurs du poste](#)).

Il existe deux variantes de suppression de l'antivirus (Agent Dr.Web et package antivirus) depuis le poste :

1. [Avec les outils standard de Windows.](#)
2. [Avec l'installateur de l'Agent Dr.Web.](#)



En cas de suppression de l'Agent et du package antivirus avec les outils standards de Windows ou avec l'installateur de l'Agent Dr.Web, il sera demandé à l'utilisateur de supprimer la Quarantaine.

Suppression avec les outils standard de Windows



Cette méthode de suppression n'est applicable que dans le cas où, durant l'installation de l'Agent Dr.Web en mode graphique, la case **Enregistrer l'Agent Dr.Web dans la liste des programmes installés** aurait été cochée.

Si l'Agent Dr.Web a été installé avec l'installateur en tâche de fond, la suppression de l'antivirus avec les outils standards ne sera possible qu'à condition que la clé `/regagent yes` ait été appliquée lors de l'installation.

Pour supprimer l'Agent Dr.Web et le package antivirus avec des outils standards de Windows, utilisez l'élément **Panneau de configuration** → **Ajout/Suppression de programmes** (pour en savoir plus, consultez le **Manuel utilisateur** pour l'**Agent Dr.Web pour Windows**).

Suppression avec l'installateur

• Module client `win-es-agent-setup.exe`

Pour désinstaller le logiciel de l'Agent Dr.Web et le package antivirus avec le module client qui est créé lors de l'installation de l'Agent Dr.Web, lancez le fichier d'installation `win-es-agent-setup.exe` avec le paramètre `/instMode remove`. Si vous souhaitez surveiller la progression du processus de suppression, utilisez le paramètre supplémentaire `/silent no`.

Le fichier de configuration `win-es-agent-setup.exe` se trouve par défaut dans le répertoire suivant :

- sous OS Windows XP et OS Windows Server 2003 :
`%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
- sous Windows Vista ou une version supérieure et sous Windows Server 2008 ou une version supérieure :
`%ALLUSERSPROFILE%\Doctor Web\Setup\`

Par exemple, sous Windows 7, où `%ALLUSERPROFILE%` correspond à `C:\ProgramData`:

```
C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode  
remove /silent no
```

• Package d'installation personnel `drweb_es_<OS>_<poste>.exe`

Pour désinstaller le logiciel de l'Agent Dr.Web et le package antivirus à l'aide du package d'installation, lancez le fichier d'installation `drweb_es_<OS>_<poste>.exe` de la version du produit qui est installée sur votre ordinateur.



- **Installeur complet drweb-*<version_de_l'agent>*-*<assemblage>*-esuite-agent-full-windows.exe**

Pour supprimer le logiciel de l'Agent Dr.Web et le package antivirus à l'aide de l'installateur complet, lancez le fichier d'installation drweb-*<version_de_l'agent>*-*<assemblage>*-esuite-agent-full-windows.exe de la version du produit qui est installée sur votre ordinateur.

- **Installeur réseau drwinst.exe**

Pour désinstaller le logiciel de l'Agent Dr.Web et le package antivirus avec l'installateur réseau en mode local, il est nécessaire de lancer dans le répertoire d'installation de l'Agent Dr.Web (par défaut — C:\Program Files\DrWeb) l'installateur drwinst.exe accompagné du paramètre /instMode remove. Si vous souhaitez surveiller la progression du processus de suppression, utilisez le paramètre /silent no.

Exemple :

```
drwinst /instMode remove /silent no
```



Au lancement du package d'installation drweb_es_*<OS>*_*<poste>*.exe, de l'installateur complet drweb-*<version_de_l'agent>*-*<assemblage>*-esuite-agent-full-windows.exe et de l'installateur réseau drwinst.exe, le module client win-es-agent-setup.exe qui effectue la suppression est lancé.

Le module client win-es-agent-setup.exe, lancé sans paramètres détermine le produit installé et se lance en mode de modification/suppression. Pour le lancer aussitôt en mode de suppression utilisez la clé /instMode remove.

6.2.2. Suppression de l'Agent Dr.Web avec le service Active Directory



La suppression de l'Agent Dr.Web est possible à condition que cette option soit autorisée sur le Serveur Dr.Web dans la section **Droits** (voir **Manuel Administrateur**, p. [Droits des utilisateurs du poste](#)).

1. Dans le panneau de configuration sous Windows, sélectionnez l'élément **Administration** puis l'élément **Active Directory - utilisateurs et ordinateurs**.
2. Dans le domaine, sélectionnez l'unité d'organisation **ESS** que vous avez créée. Depuis le menu contextuel, sélectionnez l'élément **Propriétés**. La fenêtre **Propriétés** de **ESS** s'ouvre.
3. Passez à l'onglet **Stratégie de groupe**. Sélectionnez l'élément **Stratégies ESS** dans la liste. Double cliquez sur cet élément. La fenêtre **Éditeur d'objets de stratégie de groupe** va s'ouvrir.
4. Dans l'arborescence, sélectionnez **Configuration ordinateur** → **Paramètres du logiciel** → **Installations des logiciels** → **Package**. Puis dans le menu contextuel du package contenant la distribution de l'Agent Dr.Web, sélectionnez **Toutes les tâches** → **Désinstaller** → **OK**.



5. Dans l'onglet **Stratégie de groupe**, cliquez sur **OK**.
6. Agent Dr.Web sera supprimé sur les postes lors du prochain enregistrement dans le domaine.

6.3. Suppression du Serveur de scan Dr.Web



L'opération de suppression doit être effectuée en tant que super-utilisateur (**root**).

Avant de supprimer le Serveur de scan, assurez-vous qu'il n'y a pas de postes sur le réseau antivirus qui sont configurés pour interagir avec le Serveur de scan. Sinon, ils resteront sans protection.

Pour supprimer le Serveur de scan Dr.Web

1. Sur la machine virtuelle désignée comme Serveur de scan, allez dans le dossier `/opt/drweb.com/bin`.
2. Lancez le script `uninst.sh`.
3. Le texte d'invitation à la suppression s'affichera sur l'écran. Pour commencer la procédure de suppression, répondez *Yes* ou *Y* à la question « Do you want to continue? ». Pour refuser la suppression du Serveur de scan Dr.Web, saisissez *No* ou *N*. Dans ce cas, le programme de suppression s'arrêtera.
4. Après la confirmation, la procédure de suppression de tous les paquets du Serveur de scan Dr.Web va démarrer. Les enregistrements de journal reflétant le déroulement de la suppression vont s'afficher sur l'écran.
5. À la fin du processus, le programme de suppression s'arrêtera automatiquement.

6.4. Suppression du Serveur proxy Dr.Web

Le Serveur proxy peut être supprimé par un des moyens suivants :

1. [En mode local](#).

La suppression locale est effectuée par l'administrateur sur l'ordinateur sur lequel le Serveur proxy est installé.

2. [À distance](#).

Le Serveur proxy est géré à distance depuis le Centre de gestion via LAN. La gestion à distance est disponible si le Serveur proxy est connecté au Serveur Dr.Web.



6.4.1. Suppression locale du Serveur proxy Dr.Web



Il est possible de supprimer le Serveur proxy Dr.Web depuis l'ordinateur de manière locale uniquement si l'installation a été effectuée de manière locale avec l'installateur. Sinon, il faut suivre les instructions de la section [Suppression à distance du Serveur proxy Dr.Web](#).

Sous Windows



Lors de la suppression du Serveur proxy, ses fichiers de configuration ne sont pas supprimés et restent dans le répertoire `%ALLUSERSPROFILE%\Doctor Web\`.

Le Serveur proxy Dr.Web installé sous Windows peut être supprimé avec les outils standard du système d'exploitation ou avec l'installateur.

Suppression avec les outils standard

Utilisez l'élément **Panneau de configuration** → **Ajout et suppression des programmes** (**Programmes et fonctionnalités** sous OS Windows 2008 ou une version supérieure).

Suppression avec l'installateur

• Module client proxy-setup.exe

Pour supprimer avec le module client qui est créé lors de l'installation du Serveur proxy, lancez le fichier d'installation `proxy-setup.exe` avec le paramètre `/instMode remove`. Si vous souhaitez surveiller la progression du processus de suppression, utilisez le paramètre supplémentaire `/silent no`.

Le fichier de configuration `proxy-setup.exe` se trouve par défaut dans le répertoire suivant :

- sous OS Windows XP et OS Windows Server 2003 :
`%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\drweb-win-proxy\`
- sous Windows Vista ou une version supérieure et sous Windows Server 2008 ou une version supérieure :
`%ALLUSERSPROFILE%\Doctor Web\Setup\drweb-win-proxy\`

Exemple de la commande de lancement du module sous Windows 10 où `%ALLUSERPROFILE%` correspond à `C:\ProgramData`.

```
C:\ProgramData\Doctor Web\Setup\drweb-win-proxy\proxy-setup.exe /instMode  
remove /silent no
```



- **Installeur drweb-proxy-*<version_du_package>*-*<assemblage>*-windows-nt-*<nombre_de_bits>*.exe**

Pour supprimer un Serveur proxy avec l'installateur, téléchargez depuis la [page d'installation](#) et installez le fichier d'installation drweb-proxy-*<version_de_package>*-*<assemblage>*-windows-nt-*<nombre_de_bits>*.exe. Suivez les instructions fournies.

Pour les OS de la famille UNIX



Lors de la suppression du Serveur proxy, la copie de sauvegarde des fichiers de configuration est automatiquement enregistrée dans le répertoire `/var/tmp/drwcsd-proxy`.

OS du Serveur proxy	Action
FreeBSD	Lancez le script : <code>/usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove</code>
Linux	Lancez le script : <code>/etc/opt/drweb.com/software/drweb-proxy.remove</code>

6.4.2. Suppression à distance du Serveur proxy Dr.Web

La suppression du Serveur proxy à distance est disponible uniquement si le Serveur proxy est connecté au Serveur Dr.Web (voir [Connexion du Serveur proxy Dr.Web au Serveur Dr.Web](#)).



Quand vous supprimez le compte du Serveur proxy du Centre de gestion, le Serveur proxy est supprimé du poste.


Pour supprimer un Serveur proxy

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.
2. Dans la fenêtre qui apparaît, cliquez sur le nom d'un ou de plusieurs Serveurs proxy à supprimer dans la liste hiérarchique.
3. Dans la barre d'outils, cliquez sur **Général** → **Supprimer les objets sélectionnés**.
4. La fenêtre de confirmation de la suppression va s'ouvrir. Cliquez sur **OK**.

Pour supprimer le Serveur proxy installé sur un poste lié

1. Dans le menu principal du Centre de gestion, sélectionnez l'élément **Réseau antivirus**.



2. Ouvrez la section de propriétés du poste sur lequel le Serveur proxy est installé d'une des façons suivantes :
 - a) Cliquez sur le nom du poste dans la liste hiérarchique du réseau antivirus. La section contenant les propriétés du poste va s'afficher automatiquement dans la partie droite du Centre de gestion.
 - b) Sélectionnez l'élément **Propriétés** du menu de gestion. La fenêtre contenant les propriétés du poste va s'ouvrir.
3. De la fenêtre de propriétés du poste, allez à l'onglet **Serveur proxy**.
4. Cliquez sur  **Supprimer le Serveur proxy**.
5. Cliquez sur **Enregistrer**. Le Serveur proxy sera désinstallé du poste. Le compte du Serveur proxy sera supprimé du Serveur Dr.Web.



Chapitre 7 : Mise à jour des composants de Dr.Web Enterprise Security Suite



La migration du Serveur Dr.Web de la version 12 vers la version 13 est disponible via le Centre de gestion. La procédure est décrite dans le **Manuel administrateur**, dans la rubrique [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).

Avant de procéder à la mise à jour de Dr.Web Enterprise Security Suite et de ses composants, prenez en compte les particularités suivantes :

- Avant de procéder à la mise à jour, il est fortement recommandé de vérifier les paramètres du protocole TCP/IP relatifs à l'accès à Internet. Le service DNS doit notamment être actif et correctement configuré.
- Avant la mise à niveau du Serveur Dr.Web, il est recommandé de mettre à niveau tous les composants du réseau antivirus Dr.Web Enterprise Security Suite, y compris l'Agent Dr.Web vers la version la plus récente disponible sur le SGM.
- En cas de configuration multi-serveur du réseau antivirus, il faut noter que le transfert des mises à jour entre les Serveurs Dr.Web en version 13 et les Serveurs Dr.Web en versions 6 ne s'effectue pas et la liaison entre serveurs n'est utilisée que pour le transfert des statistiques. Pour assurer le transfert des mises à jour entre serveurs, il faut mettre à niveau tous les Serveurs Dr.Web. S'il est nécessaire de laisser au sein du réseau antivirus les Serveurs Dr.Web en versions précédentes pour la connexion des Agents Dr.Web installés sur les OS qui ne sont pas supportés par la version 13 (voir [Mise à jour des Agents Dr.Web](#)), alors les Serveurs Dr.Web en versions 6 et les Serveurs Dr.Web en version 13 doivent obtenir des mises à jour séparément.
- La migration du cluster des Serveurs Dr.Web de la version 11 vers la version 13 doit être effectuée séparément, c'est-à-dire, il faut déconnecter à tour de rôle les noeuds du cluster, les connecter à la base de données embarquée et effectuer une mise à niveau. Ensuite il faut les reconnecter un par un au cluster général.
- Pour le réseau antivirus dans lequel le Serveur proxy Dr.Web est utilisé, il faut également mettre à niveau le Serveur proxy vers la version 13 en cas de mise à niveau des composants vers la version 13. Sinon, la connexion des Agents Dr.Web fournis avec la version 13 au Serveur Dr.Web en version 13 sera impossible. Il est recommandé d'effectuer la mise à niveau dans l'ordre suivant : Serveur Dr.Web → Serveur proxy Dr.Web → Agent Dr.Web.
- Lors de la suppression du Serveur Dr.Web, tous les paramètres du référentiel ne sont pas transférés dans la nouvelle version (ils sont réinitialisés aux valeurs par défaut), pourtant une copie de sauvegarde est créée. Si nécessaire, spécifiez manuellement les paramètres du référentiel après la mise à niveau du Serveur Dr.Web.
- Lors de la mise à niveau du Serveur Dr.Web vers la 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.

7.1. Mise à jour du Serveur Dr.Web sous Windows

Les options suivantes de la mise à jour sont disponibles :

- La mise à jour du Serveur Dr.Web en version 11 ou une version supérieure s'effectue automatiquement avec l'installateur.
- La mise à jour du Serveur Dr.Web en version 12 ou une version supérieure via le Centre de gestion est disponible. La procédure est décrite dans le **Manuel administrateur**, dans la rubrique [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).



S'il faut migrer de la version 6 ou 10 il faut d'abord effectuer une mise à niveau vers la version 11, ensuite - vers la version 13.

Avant de mettre à niveau le Serveur Dr.Web, merci de lire la rubrique [Mise à jour des Agents Dr.Web](#).



Pas toutes les mises à jour du Serveur Dr.Web au sein de la version 13 contiennent le fichier de distribution. Certaines d'entre elles peuvent être installées uniquement via le Centre de gestion.

Sauvegarde des fichiers de configuration

En cas de migration du Serveur Dr.Web vers la version 13 via l'installateur, les fichiers de configuration sont enregistrés dans le répertoire qui est spécifié dans le paramètre **Sauvegarder la copie de sauvegarde des données critiques du Serveur Dr.Web** lors de la mise à niveau (par défaut `<disque_d'installation>:\DrWeb Backup`).

Les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
agent.key (le nom peut varier)	clé de licence de l'Agent Dr.Web
auth-ads.conf	fichier de configuration pour l'authentification externe des administrateurs via Active Directory
auth-radius.conf	fichier de configuration pour l'authentification externe des administrateurs via RADIUS



Fichier	Description
<code>auth-ldap.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP
<code>auth-ldap-rfc4515.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
<code>auth-ldap-rfc4515-check-group.conf</code>	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory
<code>auth-ldap-rfc4515-check-group-novar.conf</code>	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié avec la vérification d'appartenance au groupe Active Directory avec l'utilisation des variables
<code>auth-ldap-rfc4515-simple-login.conf</code>	modèle du fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
<code>auth-pam.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via PAM
<code>enterprise.key</code> (le nom peut varier)	clé de licence du Serveur Dr.Web. La clé est sauvegardée uniquement si elle est présente après la mise à niveau depuis des versions antérieures. Elle n'est pas présente en cas d'installation du nouveau Serveur Dr.Web 13
<code>drwcsd-certificate.pem</code>	certificat du Serveur Dr.Web
<code>download.conf</code>	paramètres réseau pour la génération des packages d'installation de l'Agent Dr.Web
<code>drwcsd.conf</code> (le nom peut varier)	fichier de configuration du Serveur Dr.Web
<code>drwcsd.conf.distr</code>	modèle du fichier de configuration du Serveur Dr.Web avec les paramètres par défaut
<code>drwcsd.pri</code>	clé privée de chiffrement
<code>dbexport.gz</code>	exportation de la base de données
<code>drwcsd.pub</code> (le nom peut varier)	clé publique de chiffrement
<code>frontdoor.conf</code>	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur Dr.Web
<code>openssl.cnf</code>	certificat du Serveur Dr.Web pour HTTPS
<code>webmin.conf</code>	fichier de configuration du Centre de gestion



Fichier	Description
yalocator.apikey	Clé API pour l'extension Yandex Locator

Si nécessaire, copiez d'autres fichiers importants dans un autre répertoire, différent du répertoire d'installation du Serveur Dr.Web. Par exemple, les modèles de rapport sauvegardés dans le dossier `\var\templates`.

Sauvegarde de la base de données



Avant la mise à jour, assurez-vous que vous avez indiqué dans le SGBD Microsoft SQL le tri en respectant la casse (le suffixe `_CS`) et les signes diacritiques (le suffixe `_AS`). Sinon, la mise à jour automatique sera impossible.

Avant la mise à jour, assurez-vous que le SGBD utilisé est pris en charge par le Serveur Dr.Web en version 13. Sinon, la mise à jour automatique sera impossible. La liste des SGBD pris en charge se trouve dans les **Annexes**, dans l'[Annexe A. Description des paramètres du SGBD. Paramètres des pilotes du SGBD](#).

Avant la mise à niveau de Dr.Web Enterprise Security Suite, il est recommandé de sauvegarder la base de données.

Pour sauvegarder la base de données

1. Arrêter le Serveur Dr.Web.
2. Exportez la base de données vers le fichier :
 - pour le Serveur Dr.Web en version antérieure à la version 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb <dossier_de_sauvegarde>\esbase.es
```

- pour le Serveur Dr.Web à commencer par la version 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all modexecdb database-export <dossier_de_sauvegarde>\esbase.es
```

Pour les Serveurs Dr.Web utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.



Assurez-vous que l'exportation de la base de données Dr.Web Enterprise Security Suite a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le Serveur Dr.Web en cas de nécessité.



Mise à jour du Serveur Dr.Web

Pour mettre à niveau le Serveur Dr.Web, lancez le fichier de distribution.



Par défaut, la langue du système d'exploitation est sélectionnée comme la langue de l'installateur. Si nécessaire, vous pouvez modifier la langue d'installation à toutes les étapes en sélectionnant l'élément correspondant qui se trouve dans l'angle droit supérieur de la fenêtre de l'installateur.

Pour la base de données externe du Serveur Dr.Web, sélectionnez aussi **Utiliser la base de données existante** durant la mise à niveau.



Si vous projetez d'utiliser la BD Oracle via la connexion ODBC comme base de données externe, refusez l'installation du client intégré pour le SGBD Oracle dans les paramètres de l'installateur (dans la section **Support des bases de données – Pilote de la base de données Oracle**) lors de l'installation (mise à jour) du Serveur Dr.Web.

Sinon, le travail avec la BD Oracle via ODBC ne sera pas possible à cause du conflit des bibliothèques.

1. Lors de la mise à niveau de la version 11, 12 ou la mise à jour au sein de la version 13, une fenêtre va s'ouvrir vous informant sur la présence de la version précédente du Serveur Dr.Web installée et vous présentant une brève description du processus de la mise à niveau vers la nouvelle version. Pour commencer la configuration de la procédure de la mise à niveau, cliquez sur **Mettre à niveau**.
2. Une fenêtre va s'ouvrir vous proposant de créer une copie de sauvegarde des données critiques avant la suppression du Serveur Dr.Web en version précédente. Il est recommandé de cocher la case **Sauvegarde des données critiques du Serveur Dr.Web**. S'il est nécessaire, vous pouvez modifier le répertoire de copie de sauvegarde spécifié par défaut (<disque_d'installation> : \DrWeb Backup.). Pour commencer la suppression de la version précédente du Serveur Dr.Web, cliquez sur **Supprimer**.
3. Après la fin de la suppression de la version précédente du Serveur Dr.Web, l'installation de la nouvelle version commence. Une fenêtre contenant les informations sur le produit et le lien vers le texte du Contrat de licence va s'ouvrir. Après l'avoir lu, cochez la case **J'accepte les termes du Contrat de licence** et cliquez sur **Suivant**.
4. Aux étapes suivantes, la configuration du Serveur Dr.Web s'effectue avec l'utilisation de la [base de données existante](#) (de la même manière que le processus d'[Installation du Serveur Dr.Web](#) à la base des [fichiers de configuration](#) de la version précédente). L'installateur détermine automatiquement le répertoire d'installation du Serveur Dr.Web, localise les fichiers de configuration et la BD embarquée de la version précédente. Si cela est



nécessaire, vous pouvez modifier les chemins d'accès aux fichiers détectés automatiquement par l'installateur.

5. Pour commencer l'installation du Serveur Dr.Web en version 13, cliquez sur le bouton **Installer**.



Après la fin de la mise à jour des Serveurs Dr.Web du réseau antivirus, il est nécessaire :

1. Spécifier de nouveau les paramètres de chiffrement et de compression pour les Serveurs Dr.Web liés (voir le **Manuel Administrateur**, la rubrique [Configuration des liaisons entre Serveurs Dr.Web](#)).
2. Vider le cache du navigateur web utilisé pour se connecter au Centre de gestion.

7.2. Mise à jour du Serveur Dr.Web sous les OS de la famille UNIX

Vous pouvez mettre à niveau le Serveur Dr.Web vers la version 13 de plusieurs manières :

- La mise à jour du Serveur Dr.Web en version 11 ou une version supérieure pour les mêmes types de packages s'effectue automatiquement avec l'installateur pour tous les OS de la famille UNIX. Si vous voulez, vous pouvez effectuer la mise à jour manuellement.
- La mise à jour du Serveur Dr.Web en version 12 ou une version supérieure via le Centre de gestion est également disponible. La procédure est décrite dans le **Manuel administrateur**, dans la rubrique [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).



Avant de mettre à niveau le Serveur Dr.Web, merci de lire la rubrique [Mise à jour des Agents Dr.Web](#).



La mise à jour du Serveur Dr.Web au sein de la version 13 via le Centre de gestion est également disponible. La procédure est décrite dans le **Manuel Administrateur**, dans la rubrique [Mise à jour du Serveur Dr.Web et restauration depuis une copie de sauvegarde](#).

Pas toutes les mises à jour du Serveur Dr.Web au sein de la version 13 contiennent le fichier de distribution. Certaines d'entre elles peuvent être installées uniquement via le Centre de gestion.



Sauvegarde des fichiers de configuration

En cas de suppression du Serveur Dr.Web et la mise à niveau vers la version 13, les fichiers de configuration sont enregistrés dans le répertoire de sauvegarde par défaut : `/var/tmp/drwcs/`.

En cas de suppression du Serveur Dr.Web les fichiers de configuration suivants sont sauvegardés :

Fichier	Description
<code>agent.key</code> (le nom peut varier)	clé de licence de l'Agent Dr.Web
<code>auth-ldap.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP
<code>auth-ldap-rfc4515.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
<code>auth-pam.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via PAM
<code>auth-radius.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
<code>certificate.pem</code>	certificat SSL
<code>common.conf</code>	fichier de configuration (pour certains OS de la famille UNIX)
<code>dbexport.gz</code>	exportation de la base de données (créé lors de la suppression du Serveur Dr.Web avec la commande <code>drwcs.sh xmlexportdb</code>)
<code>download.conf</code>	paramètres réseau pour la génération de packages d'installation de l'Agent Dr.Web
<code>drwcsd-certificate.pem</code>	certificat du Serveur Dr.Web
<code>drwcsd.conf</code> (le nom peut varier)	fichier de configuration du Serveur Dr.Web
<code>drwcsd.pri</code>	clé privée de chiffrement
<code>drwcsd.pub</code> (le nom peut varier)	clé de chiffrement publique
<code>enterprise.key</code> (le nom peut varier)	clé de licence du Serveur Dr.Web. La clé est sauvegardée uniquement si elle est présente après la mise à niveau depuis des versions antérieures. Elle n'est pas présente en cas d'installation du nouveau Serveur Dr.Web 13



Fichier	Description
<code>frontdoor.conf</code>	fichier de configuration pour l'utilitaire du diagnostic distant du Serveur Dr.Web
<code>local.conf</code>	paramètres du journal du Serveur Dr.Web
<code>private-key.pem</code>	clé privée RSA
<code>webmin.conf</code>	fichier de configuration du Centre de gestion
<code>yalocator.apikey</code>	Clé API pour l'extension Yandex Locator

En cas de [mise à niveau automatique](#), les fichiers suivants sont enregistrés dans le répertoire de copie de sauvegarde :

Fichier	Description
<code>auth-ldap.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP
<code>auth-ldap-rfc4515.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via LDAP selon le schéma simplifié
<code>auth-pam.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via PAM
<code>auth-radius.conf</code>	fichier de configuration pour l'authentification externe des administrateurs via RADIUS
<code>db.backup.gz</code>	exportation de la base de données (créé lors de la mise à niveau du Serveur Dr.Web avec la commande <code>drwcs.sh exportdb</code>)

Sauvegarde de la base de données

Avant la mise à niveau de Dr.Web Enterprise Security Suite, il est recommandé de sauvegarder la base de données.

Pour sauvegarder la base de données

1. Arrêter le Serveur Dr.Web.
2. Exportez la base de données vers le fichier :
 - Sous FreeBSD :
 - pour le Serveur Dr.Web en version antérieure à la version 13

```
# /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
```
 - pour le Serveur Dr.Web à commencer par la version 13



```
# /usr/local/etc/rc.d/drwcsd modexecdb database-  
export /var/tmp/esbase.es
```

- Sous Linux :

- pour le Serveur Dr.Web en version antérieure à la version 13

```
# /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
```

- pour le Serveur Dr.Web à commencer par la version 13

```
# /etc/init.d/drwcsd modexecdb database-export /var/tmp/esbase.es
```

Pour les Serveurs Dr.Web utilisant une base de données externe, il est recommandé d'utiliser les outils standard fournis avec la base de données.



Assurez-vous que l'exportation de la base de données Dr.Web Enterprise Security Suite a réussi. Sans avoir une copie de sauvegarde de la BD, vous ne pourrez pas restaurer le Serveur Dr.Web en cas de nécessité.

Mise à jour automatique

La mise à jour du Serveur Dr.Web en version 11 ou une version supérieure pour les mêmes types de packages s'effectue automatiquement pour tous les OS de la famille UNIX.

Dans ce cas, les [fichiers de configuration](#) seront convertis automatiquement et placés dans les répertoires appropriés. Certains [fichiers de configuration](#) sont également sauvegardés dans le répertoire de copie de sauvegarde.

Mise à jour manuelle

Si la mise à niveau du Serveur Dr.Web en version 11 ou supérieure par-dessus le package installé n'est pas possible, il faut supprimer les versions précédentes du logiciel du Serveur Dr.Web en créant une copie de sauvegarde et installer ensuite le logiciel en version 13 d'après la copie sauvegardée.

Pour mettre à jour le Serveur Dr.Web

1. Arrêter le Serveur Dr.Web.
2. Si vous souhaitez utiliser plus tard des fichiers (à part les [fichiers](#) qui seront sauvegardés automatiquement lors de la suppression du Serveur Dr.Web à l'étape **3**), créez des copies de sauvegarde de ces fichiers manuellement. Par exemple, les modèles de rapports, etc.
3. Supprimez le logiciel du Serveur Dr.Web (voir [Suppression du Serveur Dr.Web sous les OS de la famille UNIX](#)). Il vous sera proposé d'enregistrer automatiquement des copies des [fichiers](#). Pour ce faire, indiquez un dossier ou acceptez le dossier par défaut.
4. Installez le Serveur Dr.Web en version 13 d'après la procédure standard d'installation (voir le p. [Installation du Serveur Dr.Web pour les OS de la famille UNIX](#)) basée sur la copie de sauvegarde de l'étape **3**. Tous les fichiers de configuration ainsi que la base de données



embarquée (en cas d'utilisation de la base de données embarquée) seront automatiquement convertis pour la version 13 du Serveur Dr.Web. Sans conversion automatique, la base de données (en cas d'utilisation de la base de données embarquée) et certains fichiers de configuration du Serveur Dr.Web de versions précédentes ne peuvent pas être utilisés.

En cas de sauvegarde manuelle, placez les fichiers dans les mêmes dossiers où ils se trouvaient en version précédente du Serveur Dr.Web.



Pour tous les fichiers sauvegardés de la précédente version du Serveur Dr.Web (voir l'étape 4) désignez l'utilisateur sélectionné lors de l'installation de la nouvelle version du Serveur Dr.Web (**drwcs** par défaut) comme le propriétaire des fichiers.

5. Démarrez le Serveur Dr.Web.
6. Configurez la mise à niveau du référentiel et effectuez-la.



Une fois les Serveurs Dr.Web du réseau antivirus sont mis à jour, il est nécessaire de spécifier encore une fois les paramètres de chiffrement et de compression pour les Serveurs Dr.Web liés (voir le **Manuel Administrateur**, la rubrique [Configuration des liaisons entre Serveurs Dr.Web](#)).

7.3. Mise à jour des Agents Dr.Web

La mise à jour des Agents Dr.Web après la mise à jour du logiciel du Serveur Dr.Web est décrite pour les variantes suivantes :

1. [Mise à jour des Agents Dr.Web sur les postes tournant sous Windows](#),
2. [Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Android](#),
3. [Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Linux et macOS](#).

7.3.1. Mise à jour des Agents Dr.Web sur les postes tournant sous Windows

Mise à jour des Agents Dr.Web fournis avec Dr.Web Enterprise Security Suite 10

La mise à jour des Agents Dr.Web fournis avec la version Dr.Web Enterprise Security Suite 10 se fait automatiquement.

Après le redémarrage automatique, une notification de la nécessité de redémarrage s'affiche sur le poste ; la nécessité de redémarrage est marquée dans le statut du poste après la mise à niveau. Pour terminer la mise à niveau, veuillez redémarrer le poste de manière locale ou distante via le Centre de gestion.



Au cas où le poste se connecterait au Serveur Dr.Web via le Serveur proxy Dr.Web en version 10 ou une version antérieure, avant la mise à niveau de l'Agent Dr.Web il faut mettre à niveau le Serveur proxy vers la version 13 ou supprimer le Serveur proxy.



Vu que la version 10 n'est plus pris en charge, la migration réussie de la version 10 vers la version 13 n'est pas garantie. Dans ce cas, il faut d'abord migrer vers la version 11, ensuite - vers la version 13.

Mise à niveau automatique des Agents Dr.Web fournis avec Dr.Web Enterprise Security Suite 6

Pour la mise à jour automatique il faut satisfaire aux conditions suivantes :

1. Les Agents Dr.Web doivent être installés sur les ordinateurs tournant sous Windows en versions qui prennent en charge l'installation des Agents Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0 (voir [Pré-requis système](#)).
2. En cas de la mise à jour automatique, les actions à accomplir peuvent varier en fonction des paramètres du Serveur Dr.Web :
 - a) [La mise à jour automatique](#) s'effectue si lors de la mise à niveau du Serveur Dr.Web, les clés de chiffrement et les paramètres réseau du Serveur Dr.Web précédent ont été sauvegardés.
 - b) [La mise à jour automatique requiert la configuration manuelle](#), si lors de la mise à niveau du Serveur Dr.Web, les nouvelles clé de chiffrement et les nouveaux paramètres réseau du Serveur Dr.Web ont été spécifiés.



Lors de la mise a jour automatique, prenez en compte les particularités suivantes :

1. Après la suppression de l'Agent Dr.Web, une notification sur la nécessité de redémarrage est affichée sur le poste. L'administrateur doit redémarrer le poste lui-même.
2. Après la suppression de l'ancienne version de l'Agent Dr.Web et jusqu'à l'installation de la nouvelle version, les postes ne sont pas protégés.
3. Après la mise à jour de l'Agent Dr.Web sans redémarrage du poste, le fonctionnement du logiciel antivirus est limité. Dans ce cas la protection complète antivirus n'est pas fournie. Il faut que l'utilisateur effectue la mise à jour du poste selon la demande de l'Agent Dr.Web.

La mise à jour automatique des Agents Dr.Web s'effectue conformément au schéma suivant :

1. Une fois la mise à jour est lancée, l'ancienne version de l'Agent Dr.Web est supprimée.
2. Le redémarrage du poste se fait manuellement.
3. Ensuite, s'effectue l'installation de la nouvelle version de l'Agent Dr.Web. Pour cela, une tâche est créée automatiquement dans la planification du Serveur Dr.Web.



- Après la fin de la mise à jour de l'Agent Dr.Web, le poste se connecte automatiquement au Serveur Dr.Web. Dans la section **Statut** du Centre de gestion, une notification de la nécessité de redémarrage s'affichera pour le poste mis à jour. Il est nécessaire de redémarrer le poste.

La mise à jour automatique des Agents Dr.Web avec la configuration manuelle s'effectue conformément au schéma suivant :

- Configurez manuellement les paramètres de connexion au nouveau Serveur Dr.Web et remplacez la clé publique de chiffrement sur les postes.
- Après la modification des paramètres sur le poste et la connexion du poste au Serveur Dr.Web, la mise à jour de l'Agent commencera.
- Une fois la mise à jour est lancée, l'ancienne version de l'Agent Dr.Web est supprimée.
- Le redémarrage du poste se fait manuellement.
- Ensuite, s'effectue l'installation de la nouvelle version de l'Agent Dr.Web. Pour cela, une tâche est créée automatiquement dans la planification du Serveur Dr.Web.
- Après la fin de la mise à jour de l'Agent Dr.Web, le poste se connecte automatiquement au Serveur Dr.Web. Dans la section **Statut** du Centre de gestion, une notification de la nécessité de redémarrage s'affichera pour le poste mis à jour. Il est nécessaire de redémarrer le poste.

Mise à jour automatique des Agents Dr.Web fournis avec Dr.Web Enterprise Security Suite 6

Si l'installation de la nouvelle version de l'Agent Dr.Web lors de la mise à niveau automatique a échoué pour une raison quelconque, les autres tentatives d'installation ne seront pas entreprises. Le logiciel antivirus ne sera pas installé sur le poste et un tel poste sera affiché dans le Centre de gestion comme désactivé.

Dans ce cas, l'utilisateur doit [installer l'Agent Dr.Web](#) lui-même. Après l'installation du nouvel Agent Dr.Web, il faudra fusionner l'ancien poste et le nouveau poste dans l'arborescence du réseau antivirus, dans le Centre de gestion.

Si la mise à jour n'est pas supportée

Si les Agents Dr.Web sont installés sur les postes avec les systèmes d'exploitation qui ne prennent pas en charge l'installation des Agents Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0, aucune action de mise à jour ne sera exécutée.

Les Agents Dr.Web installés sur les OS non pris en charge ne peuvent pas recevoir les mises à jour (y compris les mises à jour des bases virales) du nouveau Serveur Dr.Web. Si vous devez maintenir les Agents Dr.Web sous des OS non pris en charge, vous devez laisser dans le réseau antivirus les Serveurs Dr.Web en versions précédentes auxquels ces Agents Dr.Web sont connectés. Notez que les Serveurs Dr.Web en versions 6 et les Serveurs Dr.Web en version 13.0 doivent obtenir des mises à jour séparément.



Les recommandations sur la mise à niveau des Agents Dr.Web installés sur les postes ayant des fonctions importantes de LAN, sont disponibles dans les **Annexes**, rubrique [Mise à niveau des Agents sur les serveurs LAN](#).

7.3.2. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Android



Dr.Web Enterprise Security Suite 13.0 supporte l'interaction avec l'Agent Dr.Web pour Android en version 12.2 ou une version supérieure.

Vous pouvez mettre à jour l'Agent Dr.Web pour Android sur les appareils mobiles

1. Automatiquement. A commencer par la version 12.6.4, l'Agent Dr.Web pour Android est mis à jour automatiquement quand le Serveur Dr.Web envoie les informations sur une nouvelle version disponible. Pour configurer la mise à jour automatique, assurez-vous que dans les paramètres du référentiel du Serveur Dr.Web dans le Centre de gestion il est indiqué de mettre à jour le produit Dr.Web pour Android (**Administration** → **Configuration générale du référentiel** → **Packages d'installation Dr.Web** → **Produits d'entreprise Dr.Web**), et que la case correspondante est cochée dans les paramètres de Dr.Web pour Android dans le Centre de gestion (**Réseau antivirus** → groupe de postes ou un poste individuel tournant sous Android → **Dr.Web pour Android** → **Mises à jour** → **Vérifier la disponibilité d'une nouvelle version**).
2. Manuellement, en installant un package d'installation d'une nouvelle version sur l'appareil mobile. Pour ce faire, assurez-vous que dans les paramètres du référentiel du Serveur Dr.Web dans le Centre de gestion il est indiqué de mettre à jour le produit Dr.Web pour Android (**Administration** → **Configuration générale du référentiel** → **Packages d'installation Dr.Web** → **Produits d'entreprise Dr.Web**). Ensuite, téléchargez le package généré dans le Centre de gestion, dans les propriétés du poste ou sur la page **Administration** → **Produits d'entreprise**.



A commencer par la version 12, le Serveur Dr.Web a la possibilité de mettre à jour l'application Dr.Web Security Space pour Android si cette version de l'application a été installée depuis le Serveur Dr.Web.



7.3.3. Mise à niveau des Agents Dr.Web sur les postes tournant sous Linux et macOS

Les Agents Dr.Web installés sur les postes tournant sous les OS de la famille Linux et macOS seront connectés au Serveur Dr.Web en version 13.0, si les conditions suivantes sont satisfaites :

1. Les Agents Dr.Web doivent être installés sur les ordinateurs tournant sous les OS qui prennent en charge l'installation des Agents Dr.Web pour Dr.Web Enterprise Security Suite en version 13.0 (voir [Pré-requis système](#)).
2. Les clés de chiffrement et les paramètres réseau du Serveur Dr.Web mis à jour doivent être spécifiés sur les postes.

Après la connexion du poste au Serveur Dr.Web mis à jour :

1. Sur les postes, seules les bases virales seront mises à jour. La mise à jour automatique du logiciel antivirus ne se fait pas.
2. Si la dernière version du logiciel est installée sur les postes, aucune action supplémentaire n'est requise.
3. Si le logiciel est obsolète, téléchargez le package d'installation de la nouvelle version de l'Agent Dr.Web dans le Centre de gestion, dans les paramètres du poste ou sur la [page d'installation](#). Mettez à niveau manuellement le logiciel des postes comme cela est décrit dans les **Manuels utilisateur** correspondants.

7.4. Mise à jour du Serveur proxy Dr.Web

7.4.1. Mise à jour du Serveur proxy Dr.Web lors de son fonctionnement

La mise à jour du Serveur proxy peut être effectuée automatiquement au cours de son fonctionnement.



Si le Serveur Dr.Web sous l'OS de la famille UNIX a été mis à niveau depuis la version 11.0 ou 11.0.1, la mise à jour automatique du Serveur proxy Dr.Web sera impossible. Pour enlever cette limitation, il faut supprimer manuellement le suffixe `^win.*` dans le champ **Mettre à jour seulement les fichiers suivants** Administration → Configuration détaillée du référentiel → Serveur proxy Dr.Web → Synchronisation.

En cas de l'installation initiale du Serveur Dr.Web en version 11.0.2, il n'y a aucune limitation de mise à jour automatique du Serveur proxy.



La planification de la mise à jour dépend des paramètres de la mise en cache proactive du Serveur proxy :

1. Si le Serveur proxy n'est pas inclus dans la liste de la mise en cache proactive (même si la mise en cache n'est pas utilisée), les mises à jour du Serveur proxy seront téléchargées et installées automatiquement conformément à la planification de la mise à jour automatique.
2. Si le Serveur proxy est inclus dans la liste de la mise en cache proactive, les mises à niveau du Serveur proxy seront automatiquement téléchargés conformément à la planification de la mise en cache proactive. Si une nouvelle révision du Serveur proxy est reçue, la mise à niveau vers cette révision sera effectuée conformément à la planification automatique.

Vous pouvez configurer la mise à jour automatique par l'un des moyens suivants :

- Via les paramètres du Serveur proxy, dans le Centre de gestion du Serveur gérant Dr.Web, dans la section **Mises à jour**. Pour en savoir plus, consultez le **Manuel Administrateur**, la rubrique [Configuration distante du Serveur proxy](#).
- Via le fichier de configuration du Serveur proxy `drwcsd-proxy.conf`. Vous trouverez la description détaillée dans le document **Annexes**, [F4. Fichier de configuration du Serveur proxy Dr.Web](#).

7.4.2. Mise à jour du Serveur proxy Dr.Web via l'installateur

Fichiers de configuration du Serveur proxy

Fichiers de configuration du Serveur proxy en version 11 et supérieure :

Fichier	Description
<code>drwcsd-proxy.conf</code>	fichier de configuration du Serveur proxy (voir les Annexes , p. Mise à niveau des Agents Dr.Web sur les postes tournant sous l'OS Linux et macOS)
<code>drwcsd-proxy.auth</code>	données d'identification (ID et mot de passe) pour l'accès au Serveur Dr.Web.
<code>drwcsd-proxy-trusted.list</code>	liste des certificats de confiance des Serveurs Dr.Web
<code>drwcsd-proxy-signed.list</code>	liste des certificats signés du Serveur proxy
<code>drwcsd-proxy.pri</code>	clé privée de chiffrement du Serveur proxy



Mise à niveau du Serveur proxy sous Windows

La mise à niveau se fait automatiquement à l'aide de l'installateur.

Pour mettre à niveau le Serveur proxy en version 11 ou supérieure

1. Lancez le fichier de distribution du Serveur proxy.
2. Une fenêtre va s'ouvrir vous informant sur la présence du logiciel installé du Serveur de la version précédente et vous proposant la mise à niveau vers la nouvelle version. Pour commencer la configuration de la procédure de la mise à niveau, cliquez sur **Upgrade**.
3. Une fenêtre s'affiche vous informant de la suppression du Serveur proxy de la version précédente. Pour commencer la suppression, cliquez sur **Uninstall**.
4. Après la fin de la suppression de la version précédente du Serveur proxy, l'installation d'une nouvelle version commence. Une fenêtre d'informations sur le produit s'ouvre. Cliquez sur **Next**.
5. Aux étapes suivantes, la configuration du Serveur proxy est effectuée de la même manière que le processus d'[Installation du Serveur proxy Dr.Web](#) à la base des [fichiers de configuration](#) de la version précédente. L'installateur détermine automatiquement le répertoire d'installation du Serveur proxy et localise les fichiers de configuration de la version précédente. Si cela est nécessaire, vous pouvez modifier les paramètres de fichiers qui sont trouvés automatiquement par l'installateur.
6. Pour commencer l'installation du Serveur proxy, cliquez sur le bouton **Install**.

Mise à niveau du Serveur proxy sous les OS de la famille UNIX

Pour mettre à niveau le Serveur proxy en version 11.0 ou antérieure



Lors de la mise à niveau du Serveur proxy, les [fichiers de configuration](#) sont supprimés. Si nécessaire, sauvegardez les fichiers de configuration manuellement avant la mise à niveau.

1. Pour lancer la mise à niveau, lancez le fichier de distribution du Serveur proxy :
`./<fichier_de_distribution>.tar.gz.run`
2. Après la mise à niveau, transférez manuellement les paramètres de [fichiers de configuration](#) sauvegardés avant la mise à niveau vers les nouveaux fichiers de configuration, si cela est nécessaire.

Pour mettre à niveau le Serveur proxy en version 11.0.1

1. Pour lancer la mise à niveau, lancez le fichier de distribution du Serveur proxy :
`./<fichier_de_distribution>.tar.gz.run`
2. Lors de la suppression de la version précédente, les [fichiers de configuration](#) du Serveur proxy seront sauvegardés automatiquement.



3. Si nécessaire, vous pouvez utiliser les fichiers de configuration de l'installation précédente du Serveur proxy, enregistrés lors de la sauvegarde :
 - Pour utiliser la copie de sauvegarde enregistrée par défaut dans le dossier `/var/tmp/drwcsd-proxy`, cliquez sur ENTRER.
 - Pour utiliser une copie de sauvegarde se trouvant dans un autre dossier, indiquez le chemin d'accès manuellement.
 - Vous pouvez également installer le Serveur proxy avec les paramètres par défaut sans utiliser la copie de sauvegarde de la configuration de l'installation précédente. Pour ce faire, cliquez sur 0.



Référence

A

- Active Directory
 - généralités 53
 - installation de l'Agent 95
 - suppression de l'Agent 120
- Agent
 - installation 65, 78
 - installation, à distance 82, 95
 - installation, Active Directory 95
 - installation, en mode local 70
 - mise à jour 134
 - suppression, Active Directory 120
 - suppression, pour Windows 117

C

- certificat 49
- chiffrement
 - généralités 43
- clé privée 49
- clé publique 49
- clés
 - chiffrement 49
 - de licence 33
 - démo 34
- clés de démo 34
- clés de licence
 - réception 33
- codes d'erreur
 - installation 113
- compression du trafic 43
- compte
 - poste 72
 - Serveur proxy 103
- création
 - compte, poste 72
 - compte, Serveur proxy 103

D

- distribution 31

E

- enregistrement
 - produit Dr.Web 33

I

- icônes
 - scanner réseau 84
- installateur
 - composition 67
 - installation 78
 - suppression 119
 - types 67
- installation 65
 - Agent 65
 - codes d'erreur 113
 - NAP Validator 101
 - package antivirus 65
 - Serveur proxy 102
 - Serveur, pour les OS UNIX 64
 - Serveur, sous Windows 57
- installation de l'Agent 65
 - à distance 82, 95
 - Active Directory 95
 - en mode local 70
 - installateur 78
 - package d'installation de groupe 76
 - package d'installation personnel 72

M

- mise à jour
 - Agent 134
 - Serveur, pour les OS UNIX 130
 - Serveur, sous Windows 126

N

- NAP Validator
 - installation 101

O

- octroi de licence 33

P

- package antivirus
 - installation 65
 - suppression 117
- package d'installation
 - composition 67
 - de groupe 67, 76
 - personnel 67, 72



Référence

- package d'installation
 - types, comparaison 70
- package d'installation de groupe
 - généralités 67
 - installation 76
- package d'installation personnel
 - généralités 67
 - installation 72
- page d'installation 67
- poste
 - compte, création 72
- Protocole SRV 42
- chiffrement 43
- compression 43

R

- réseau antivirus
 - création 35

S

- scanner réseau 82
- Serveur Dr.Web
 - installation, pour les OS UNIX 64
 - installation, sous Windows 57
 - mise à jour, sous OS UNIX 130
 - mise à jour, sous Windows 126
 - suppression, sous les OS UNIX 115
 - suppression, sous Windows 115
- Serveur proxy
 - compte 103
 - connexion au Serveur Dr.Web 110
 - installation 102
 - suppression 121
- service de détection du Serveur Dr.Web 41
- suppression
 - Agent 117
 - composants 117
 - package antivirus 117
 - Serveur proxy 121
 - Serveur, sous les OS UNIX 115
 - Serveur, sous Windows 115
- suppression de l'Agent
 - Active Directory 120
 - installateur 119
 - pour Windows 117

T

- trafic

