Dr.WEB

Enterprise Security Suite

Instrucciones para desplegar la red antivirus

Dr.Web Enterprise Security Suite
Versión 10.0
Instrucciones para desplegar la red antivirus
12/26/2016

Doctor Web, Oficina central en Rusia

125040

Rusia, Moscú

3-a calle de Yamskoye pole, nº 2, edificio 12A

Página web: http://www.drweb.com/

Teléfono: +7 (495) 789-45-87

Puede obtener información sobre las delegaciones y oficinas regionales en la página web oficial de la empresa.

Doctor Web

Doctor Web es un desarrollador ruso de sistemas de seguridad informática.

Doctor Web ofrece soluciones eficaces antivirus y antispam tanto para organizaciones estatales y grandes empresas como para el uso personal.

Las soluciones antivirus de la familia Dr.Web llevan desarrollándose desde 1992 y muestran constantemente unos resultados excelentes en la detección de programas maliciosos de acuerdo con las normas de seguridad de todo el mundo.

Sus certificados y premios, así como la extensa distribución geográfica de sus usuarios, son una prueba de la excepcional confianza mostrada hacia los productos de la empresa.

¡Agradecemos a los usuarios su apoyo a las soluciones de la familia Dr.Web!

Contenido

Capítulo 1: Enterprise Security Suite de Dr.Web

1.1. Introducción

1.1.1. Designación del documento

Las instrucciones para desplegar la red antivirus contienen una breve información sobre la instalación y la configuración inicial de los componentes de la red antivirus. Para obtener información detallada consulte la documentación del administrador.

La documentación del administrador de la red antivirus Enterprise Security Suite de Dr.Web se compone de las siguientes partes principales:

1. **Manual de instalación** (archivo **drweb-esuite-10-install-manual-es.pdf**)
2. **Manual del administrador** (archivo **drweb-esuite-10-admin-manual-en.pdf**)
3. **Anexos** (archivo **drweb-esuite-10-appendices-en.pdf**)

En la documentación figuran enlaces cruzados entre los documentos mencionados. En el caso de que los documentos se descarguen en un ordenador local, los enlaces cruzados únicamente funcionarán si los documentos se encuentran en un mismo directorio y conservan sus nombres originales.

Antes de leer los documentos, asegúrese de que se trata de la última versión de los Manuales. Los manuales se actualizan constantemente y la última versión se puede encontrar en la página web oficial de la compañía Doctor Web https://download.drweb.ru/doc/.

1.1.2. Signos convencionales

En este manual se utilizan los signos indicados en la tabla 1-1.

Tabla 1-1. Signos convencionales

Signo	Comentario
	Nota o indicación importante.
	Advertencia sobre posibles errores y aspectos importantes que deben tenerse en cuenta.
Red antivirus	Nuevo término o acento sobre un término en las descripciones.
<IP-address>	Campo para reemplazar los nombres de funciones por valores reales.
Guardar	Nombres de los botones de la pantalla, ventanas, opciones del menú y otros elementos de la interfaz del programa.
CTRL	Signos de las teclas del teclado.
`C:\Windows\`	Nombres de los archivos y los directorios, fragmentos del código del programa.
Anexo A	Referencias cruzadas a partes del documento o hiperenlaces a recursos externos.

1.2. Acerca del producto

Enterprise Security Suite de Dr.Web está previsto para organizar y administrar una protección antivirus integral, unificada y fiable tanto en una red interna de una empresa, incluyendo dispositivos móviles, como en los ordenadores personales de los trabajadores.

El conjunto de los ordenadores y dispositivos móviles en los que están instalados los componentes interrelacionados de Enterprise Security Suite de Dr.Web forma una única *red antivirus*.

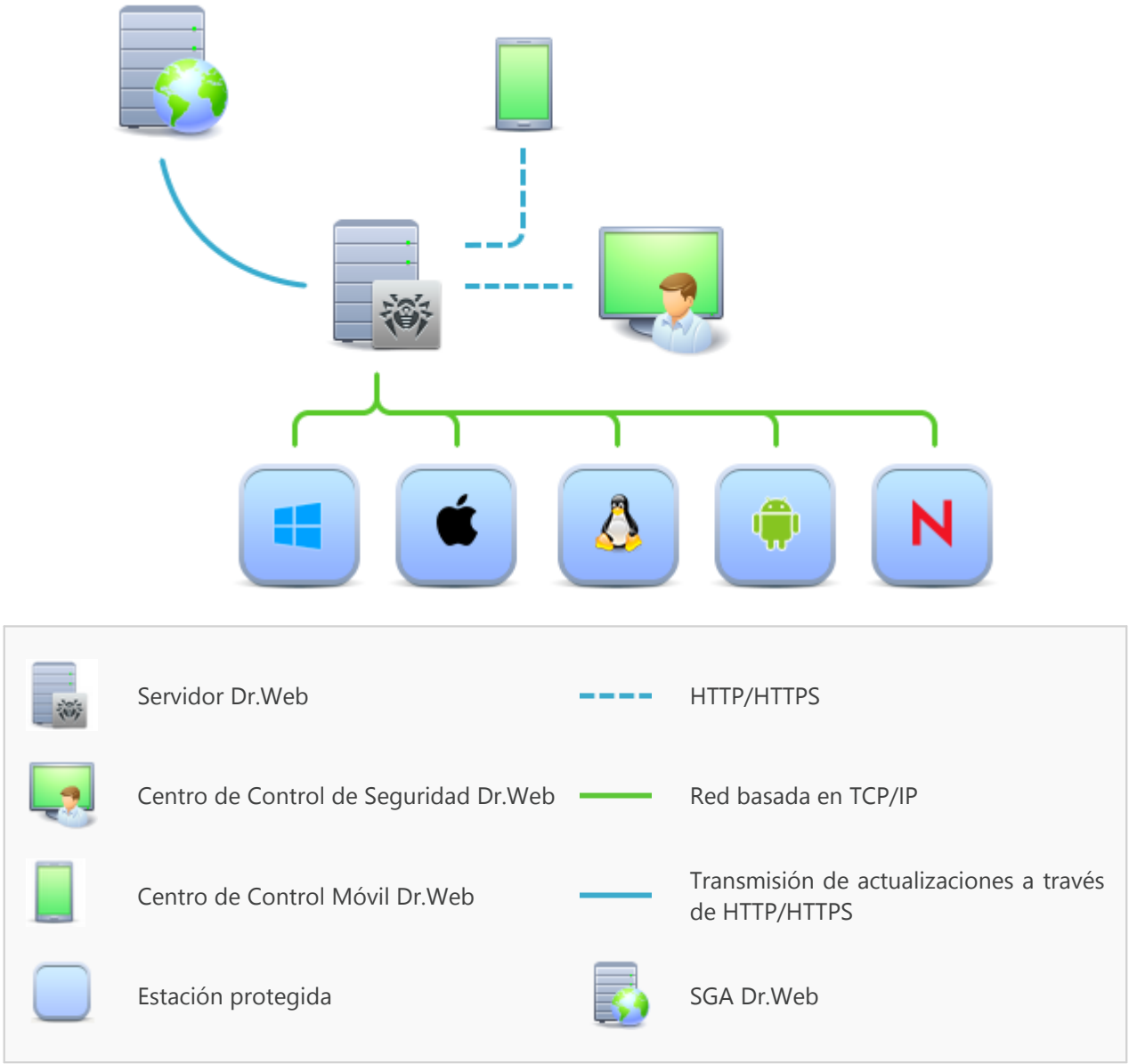

Imagen 1-1. Estructura lógica de la red antivirus

La red antivirus de Enterprise Security Suite de Dr.Web tiene una arquitectura *cliente-Servidor*. Sus componentes se instalan en los ordenadores y dispositivos móviles de los usuarios y administradores, así como en los ordenadores que desempeñan la función de Servidores de la red local. Los componentes de la red antivirus se intercambian información utilizando los protocolos de

red TCP/IP. El software del antivirus en las estaciones protegidas puede instalarse (y ser administrada por ellas) tanto a través de la red local como a través de internet.

Servidor de protección centralizada

El Servidor de protección centralizada se instala en uno de los ordenadores de la red antivirus y la instalación es posible en cualquier ordenador, no solo en el ordenador que cumple la función de Servidor de la red local. Los requisitos principales para este ordenador se indican en el punto Requisitos del sistema.

La naturaleza multiplataforma del software del Servidor permite utilizar como Servidor un ordenador con uno de los siguientes sistemas operativos:

- SO Windows®,
- SO de la familia UNIX® (Linux®, FreeBSD®, Solaris™).

El Servidor de protección centralizada conserva las distribuciones de los paquetes antivirus para los distintos SO de los ordenadores protegidos, las actualizaciones de las bases de virus y de los paquetes antivirus, las claves de licencia y la configuración de los paquetes antivirus de los ordenadores protegidos. El Servidor obtiene la actualización de los ordenadores de la red antivirus y de las bases de virus a través de internet desde los Servidores del Sistema Global de Actualizaciones y la propaga a las estaciones protegidas.

Base de datos unificada

La base de datos unificada se conecta al Servidor de protección centralizada y conserva datos estadísticos sobre los eventos de la red antivirus, la configuración del Servidor, los parámetros de las estaciones protegidas y los componentes antivirus instalados en las estaciones protegidas.

Centro de control de protección centralizada

El Centro de control de protección centralizada se instala automáticamente junto con el Servidor y ofrece una interfaz web para administrar el Servidor y la red antivirus de forma remota mediante la edición de la configuración del Servidor y de los ordenadores protegidos almacenada en el Servidor y en los ordenadores protegidos.

El Centro de control puede abrirse en cualquier ordenador que tenga acceso por red al Servidor. Puede utilizarse en prácticamente cualquier sistema operativo y ofrece funcionalidad completa en los siguientes exploradores web:

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

La lista de las opciones de uso disponibles se indica en los Requisitos del sistema.

El Servidor web, que se instala automáticamente con el Servidor, forma parte del Centro de Control de Seguridad Dr.Web. El Servidor web se encarga del trabajo con las páginas del Centro de control y con las conexiones de red del cliente.

Centro móvil de control de protección centralizada

El Centro móvil de control, previsto para su instalación e inicio en dispositivos móviles con iOS y SO Android, es un componente que se ofrece por separado. Los requisitos principales para esta aplicación se indican en el punto Requisitos del sistema.

La conexión del Centro móvil de control al Servidor se realiza en base a las cuentas de usuario de administrador de la red antivirus, con un protocolo cifrado.

Puede descargar el Centro móvil de control desde el Centro de control o directamente desde la App Store y Google Play.

Protección de las estaciones de la red

En los ordenadores y dispositivos móviles protegidos de la red se instala el módulo de control (Agente) y el paquete antivirus para cada sistema operativo.

La naturaleza multiplataforma del software permite llevar a cabo una protección antivirus de ordenadores y dispositivos móviles con los siguientes sistemas operativos:

- SO Windows®,
- SO de la familia UNIX®,
- OS X®,
- SO Android,
- SO Novell® NetWare®.

Como estaciones protegidas pueden utilizarse tanto los ordenadores de usuario como los Servidores de la red local. En particular, existe compatibilidad con la protección antivirus del sistema Microsoft® Outlook®.

El módulo de administración realiza regularmente actualizaciones de los componentes antivirus y de las base s de virus del Servidor y envía al Servidor información sobre los eventos de virus en un ordenador protegido.

En caso de que el Servidor de protección centralizada no esté disponible, es posible actualizar las bases de virus de las estaciones protegidas directamente a través de internet desde el Sistema Global de Actualizaciones.

Suministro de la conexión entre los componentes de la red antivirus

Para garantizar una conexión estable y segura entre los componentes de una red antivirus existen las siguientes opciones:

Servidor proxy de Dr.Web

El Servidor proxy puede conectarse opcionalmente a la red antivirus. La tarea principal del Servidor proxy es garantizar la conexión entre el Servidor y las estaciones protegidas en caso de que no se pueda establecer un acceso directo.

Compresión del tráfico

Existen algoritmos especiales de compresión para la transferencia de datos entre los componentes de la red antivirus, lo cual garantiza un tráfico de red mínimo.

Cifrado del tráfico

Ofrece la opción de cifrar la transferencia de datos entre los componentes de la red antivirus, lo cual garantiza un mayor nivel de protección.

Opciones avanzadas

NAP Validator

NAP Validator se suministra como componente adicional y permite utilizar la tecnología Microsoft Network Access Protection (NAP) para comprobar el funcionamiento del software de las estaciones de trabajo protegidas.

Cargador del repositorio

El cargador del repositorio Dr.Web se suministra como componente adicional y permite descargar los productos de Enterprise Security Suite de Dr.Web desde el Sistema Global de Actualizaciones. Puede utilizarse para descargar actualizaciones de los productos de Enterprise Security Suitede Dr.Web para copiar las actualizaciones en un Servidor no conectado a internet.

1.3. Requisitos del sistema

Para el funcionamiento del Servidor Dr.Web es necesario:

Componente	Requisitos

Procesador y sistema operativo	Los siguientes sistemas operativos instalados en ordenadores con sus CPU correspondientes son compatibles:
	• CPU compatible con la instrucción SSE2 y con 1,3 GHz de frecuencia y superior:
	  ▫ SO Windows;
	  ▫ SO Linux;
	  ▫ SO FreeBSD;
	  ▫ SO Solaris x86.
	• CPU V9 UltraSPARC IIIi y superior:
	  ▫ SO Solaris Sparc.
	La lista completa de los SO soportados se encuentra en el documento **Anexos**, en el Anexo A.

Memoria de acceso aleatorio	• Requisitos mínimos: 1 GB. • Requisitos recomendados: 2 GB y más.

Componente	Requisitos
Espacio en el disco duro	mínimo 12 GB: hasta 8 GB para la base de datos incorporada (directorio de la instalación), hasta 4 GB en el directorio temporal del sistema (para los archivos de trabajo).

Para el uso del Centro de Control de Seguridad Dr.Web se requiere:

a) Explorador web:

Explorador web	Soporte
Windows Internet Explorer 8 y superior	Compatible con
Mozilla Firefox 25 y superior	
Google Chrome 30 y superior	
Opera® 10 y superior	Se permite el uso pero no se garantiza la posibilidad del funcionamiento.
Safari® 4 y superior	

b) Para conseguir la funcionalidad total del Centro de control es necesario instalar la extensión del Centro de Control de Seguridad Dr.Web. La extensión se suministra junto con la distribución del Servidor y se instala mediante solicitud del explorador durante el proceso de trabajo con los elementos del Centro de control que requieren cargar la extensión (para el Escáner de red, en la instalación remota de los componentes del antivirus). La instalación de la extensión está disponible en los exploradores web Windows Internet Explorer 8 y superior o Mozilla Firefox 25 y superior.

c) La resolución recomendada de la pantalla para utilizar el Centro de control es de 1280x1024 px.

Para el uso del Centro de Control móvil Dr.Web se requiere:

Los requisitos varían dependiendo del sistema operativo en el que está instalada la aplicación:

Sistema operativo	Requisitos	
	Versión del sistema operativo	Dispositivo
iOS	iOS® 7 y superior	Apple® iPhone® Apple® iPad®
Android	Android 4.0 y superior	–

Para el uso del Agente Dr.Web y del paquete antivirus completo es necesario:

Los requisitos varían dependiendo del sistema operativo en el que está instalada la solución antivirus (la lista completa de SO soportados se indica en el documento **Anexos**, en el Anexo A. Lista completa de versiones soportadas de SO):

- SO Windows:

Componente	Requisitos
Procesador	CPU con 1 GHz de frecuencia y superior.
Memoria de acceso aleatorio libre	512 MB como mínimo.
Espacio libre en el disco duro	1 GB para los archivos ejecutables + espacio adicional para los historiales de funcionamiento y los archivos temporales.

- SO de la familia Linux:

Componente	Requisitos
Procesador	Es compatible con los procesadores con arquitectura y sistema de comandos Intel/AMD: 32 bits (IA-32, x86); 64 bits (x86-64, x64, amd64).
Memoria de acceso aleatorio libre	512 MB como mínimo.
Espacio libre en el disco duro	400 MB como mínimo de espacio libre en disco en la unidad donde se encuentre el directorio del antivirus.

- OS X, SO Android y SO Novell NetWare: los requisitos para la configuración coinciden con los requisitos para el sistema operativo.

1.4. Configuración de entrega

La distribución de Dr.Web Enterprise Security Suite se entrega dependiendo del SO del Servidor Dr.Web escogido:

1. Para SO de la familia UNIX: archivos en formato `run`:

Nombre del archivo	Componente
`drweb-esuite-server-10.00.0-<compilación>-<versión_SO>.run`	Distribución básica del Servidor Dr.Web*
`drweb-esuite-extra-10.00.0-<compilación>-<versión_SO>.run`	Distribución avanzada del Servidor Dr.Web

Nombre del archivo	Componente
drweb-esuite-proxy-10.00.0-<*compilación*>-<*versión_SO*>.run	Servidor proxy

2. Para SO Windows: archivos ejecutables:

Nombre del archivo	Componente
drweb-esuite-server-10.00.0-<*compilación*>-<*versión_SO*>.exe	Distribución básica del Servidor Dr.Web*
drweb-esuite-extra-10.00.0-<*compilación*>-<*versión_SO*>.exe	Distribución avanzada del Servidor Dr.Web
drweb-esuite-proxy-10.00.0-<*compilación*>-<*versión_SO*>.msi	Servidor proxy
drweb-esuite-agent-activedirectory-10.00.0-<*compilación*>.msi	Agente Dr.Web para Active Directory
drweb-esuite-modify-ad-schema-10.00.0-<*compilación*>-<*versión_SO*>.exe	Utilidad para modificar el esquema de Active Directory
drweb-esuite-aduac-10.00.0-<*compilación*>-<*versión_SO*>.msi	Utilidad para cambiar los atributos de los objetos de Active Directory
drweb-esuite-napshv-10.00.0-<*compilación*>-<*versión_SO*>.msi	NAP Validator

***La distribución básica del Servidor Dr.Web está formada por los siguientes componentes:**

- Software del Servidor Dr.Web para el SO correspondiente,
- Software de los Agentes de Dr.Web y de los paquetes antiviruspara los ordenadores con SO Windows,
- Software del Centro de Control de Seguridad Dr.Web,
- bases de virus,
- Extensión del Centro de Control de Seguridad Dr.Web,
- Extensión de Dr.Web Server FrontDoor,
- documentación, modelos y ejemplos.

Junto a la distribución se entregan números de serie que deberá registrar para obtener los archivos con las claves de licencia.

Capítulo 2: Crear una red antivirus

Guía breve para desplegar la red antivirus

1. Prepare un plan de estructura de la red antivirus, incluya en él todos los ordenadores y dispositivos móviles protegidos.

   Escoja el ordenador que desempeñará las funciones de Servidor Dr.Web. En una red antivirus puede haber varios Servidores Dr.Web. Los detalles de esta configuración se describen en el **Manual del administrador**, punto Propiedades de una red con varios Servidores Dr.Web.

   > El Servidor Dr.Web se puede instalar en cualquier ordenador, no solo en el ordenador que desempeña las funciones de Servidor de la red local. Los requisitos básicos para este ordenador se indican en el punto Requisitos del sistema.
   >
   > En todas las estaciones protegidas, incluyendo los Servidores de la red local, debe instalarse la misma versión del Agente Dr.Web. Las diferencias se recopilan en una lista de componentes antivirus instalados definida por la configuración del Servidor.

   Para instalar el Servidor Dr.Web y el Agente Dr.Web es necesario un único acceso (físico o con el uso de medios de control remoto y de inicio de programas) a los ordenadores implicados. El resto de las acciones se llevan a cabo desde el puesto de trabajo del administrador de la red antivirus (incluso desde fuera de la red local) y no requieren el acceso a los Servidores Dr.Web ni a las estaciones de trabajo.
2. Según el plan preparado, defina qué productos necesita instalar para qué sistemas operativos en cada unidad de la red. Encontrará información detallada sobre los productos ofrecidos en la sección Configuración de entrega.

   Puede adquirir todos los productos necesarios comprando el paquete de Enterprise Security Suite de Doctor Web o descargarlos desde la página web de la compañía Doctor Web https://download.drweb.ru/.

   > Los Agentes de Dr.Web para ordenadores con SO Android, Linux, y OS X también pueden instalarse a partir de los paquetes para productos independientes y conectarse posteriormente a un Servidor Dr.Web centralizado. La descripción de la configuración correspondiente para los Agentes se indica en el **Manual de instalación**, punto Instalación del Agente de Dr.Web con la ayuda del paquete de instalación personal.
3. Instale la distribución básica del Servidor Dr.Web en el ordenador u ordenadores escogidos. El proceso de instalación se describe en el **Manual de instalación**, punto Instalación del Servidor Dr.Web.

   Junto con el Servidor se instalará el Centro de Control de Seguridad Dr.Web.

   Por defecto, el Servidor Dr.Web se ejecuta automáticamente tras la instalación y después de cada reinicio del sistema operativo.

4. Si una red antivirus incluye estaciones protegidas con SO Android, Linux y OS X, instale la distribución avanzada del Servidor Dr.Web en todos los ordenadores que tienen instalada la distribución básica del Servidor.
5. Si lo necesita, instale y configure el Servidor proxy. La descripción del proceso se encuentra en el **Manual de instalación**, punto Instalación del Servidor proxy.
6. Para configurar el Servidor y el software del antivirus en las estaciones es necesario conectarse al Servidor mediante el Centro de Control de Seguridad Dr.Web.

   

   El Centro de Control puede abrirse en cualquier ordenador y no solo en el ordenador en el que está instalado el Servidor. Basta con conectar por red el ordenador que tiene instalado el Servidor.

   El Centro de Control está disponible en la dirección:

   `http://<Dirección_Servidor>:9080`

   o

   `https://<Dirección_Servidor>:9081`

   en la que como *<Dirección_Servidor>* deberá indicar la dirección IP o el nombre de dominio del ordenador en el que está instalado el Servidor Dr.Web.

   En la ventana de diálogo de la solicitud de autorización introduzca el nombre de registro o la contraseña del administrador.

   El nombre del administrador por defecto es **admin**.

   Contraseña:

   - para SO Windows: la contraseña establecida durante la instalación del Servidor.
   - para SO de la familia UNIX: **root**.

   

   Para un Servidor con SO de la familia UNIX cambie la contraseña del administrador por defecto durante la primera conexión al Servidor.

   Cuando se logra conectar con el Servidor se abre la ventana principal del Centro de Control (puede encontrar una descripción detallada en el **Manual del administrador**, en el punto Centro de Control de Seguridad Dr.Web).
7. Realice la configuración inicial del Servidor (puede encontrar una descripción detallada de la configuración del Servidor en el **Manual del administrador**, en el Capítulo 7: Configuración del Servidor Dr.Web):
   a. En la sección Administrador de licencias añada una o varias claves de licencia y extiéndalas a los grupos correspondientes, especialmente al grupo **Everyone**. Este paso es obligatorio si durante la instalación del Servidor no se ha introducido una clave de licencia.
   b. En la sección Configuración general del repositorio indique qué componentes de la red antivirus se actualizarán con el SGA Dr.Web. En la sección Estado del repositorio actualice los productos del repositorio del Servidor. La actualización puede tardar un tiempo. Espere hasta el final del proceso de actualización antes de continuar con la configuración.
   c. En la página **Administración** → **Servidor Dr.Web** encontrará información sobre la versión del Servidor. En caso de que exista una nueva versión, actualice el Servidor tal y como se

describe en el **Manual del administrador**, punto Actualización del Servidor Dr.Web y recuperación de una copia de seguridad.

d. En caso de necesidad, configure Conexiones de red para cambiar la configuración de red por defecto utilizada en la interacción de todos los componentes de la red antivirus.

e. En caso de necesidad, configure una lista de administradores del Servidor. También está disponible la autentificación externa de administradores. Encontrará más detalles en el **Manual del administrador**, en el Capítulo 4: Administradores de la red antivirus.

f. Antes de empezar a utilizar el software del antivirus se recomienda cambiar la configuración del directorio de copias de seguridad de datos críticos del Servidor (consulte el **Manual del administrador**, punto Configuración de la programación del Servidor Dr.Web). Es recomendable ubicar este directorio en otro disco local para reducir la probabilidad de perder simultáneamente los archivos del software del Servidor y los de la copia de seguridad.

8. Establezca los ajustes y la configuración de el software del antivirus para las estaciones de trabajo (encontrará información más detallada sobre la configuración de los grupos y las estaciones en el **Manual del administrador**, en el Capítulo 5 y el Capítulo 6):

   a. Si lo necesita, puede crear grupos de usuarios de cada estación.

   b. Establezca la configuración del grupo **Everyone** y de los grupos de usuarios creados. En particular, configure la sección de los componentes instalados.

9. Instale el software del Agente Dr.Web en las estaciones de trabajo.

   En la sección Archivos de instalación encontrará una lista de los archivos suministrados para instalar el Agente. Escoja la opción de instalación adecuada para usted dependiendo del sistema operativo de la estación, la opción de realizar una instalación remota, las opciones de configuración del Servidor durante la instalación del Agente, etc. Por ejemplo:

   - Para la instalación local pueden utilizarse los paquetes de instalación que deben crearse mediante el Centro de Control o bien los instaladores que puede obtener directamente desde la página de instalación.
   - Para la instalación en una estación con SO Windows en red mediante el Centro de Control es necesario establecer una extensión del navegador para el Centro de Control, ejecutar el navegador como administrador e iniciar la instalación remota en las estaciones requeridas.
   - También se puede instalar en red a través del servicio Active Directory. Para ello se utiliza el instalador del Agente Dr.Web para redes con Active Directory, suministrado junto con el paquete de instalación del Servidor.
   - La instalación en una estación con SO Android, Linux o OS X puede realizarse de forma local según las normas generales. Además, un producto independiente ya instalado puede conectarse al Servidor tras la configuración correspondiente.

10. Inmediatamente después de instalarse en los ordenadores, los Agentes establecen automáticamente conexión con el Servidor. La autorización de las estaciones del antivirus en el Servidor se lleva a cabo según la política escogida (consulte el **Manual del administrador**, punto Política de conexión de las estaciones):

    a. En caso de realizar instalación desde los paquetes de instalación, así como en caso de que se configure la confirmación automática del Servidor, las estaciones obtendrán automática-

mente el registro durante la primera conexión al Servidor y no necesitarán confirmación posteriormente.

b. En caso de realizar la instalación desde los instaladores y de que se configure una confirmación manual del acceso del administrador, será necesario confirmar manualmente cada estación de trabajo nueva para su registro en el Servidor. Las nuevas estaciones de trabajo no se conectarán automáticamente y el Servidor las añadirá al grupo de unidades nuevas.

11. Una vez conectada al Servidor y configurada una estación, en ella se instalará el conjunto correspondiente de componentes del paquete antivirus escogido en la configuración delgrupo inicial de la estación.

> Para finalizar la instalación de los componentes de la estación de trabajo es necesario reiniciar el ordenador.

12. También es posible configurar la estación y el software del antivirus después de la instalación (encontrará información más detallada sobre la configuración de los grupos y las estaciones en el **Manual del administrador**, en el Capítulo 6).

Anexo A. Licencia

Los derechos de licencia de Enterprise Security Suite de Dr.Web se regulan con la ayuda de un archivo de clave de licencia.

El archivo de la clave tiene un formato protegido contra la edición mediante un mecanismo de firma electrónica. La edición de este archivo lo vuelve inservible. Para evitar la corrupción accidental del archivo de la clave, no se debe modificar el archivo clave y/o guardarlo después de verlo en un editor de texto.

La composición y el precio de una licencia de uso de la solución antivirus Enterprise Security Suite de Dr.Web dependen del número de estaciones protegidas de la red (incluidos los Servidores que forman parte de la red de Enterprise Security Suite de Dr.Web como estaciones protegidas).

Es obligatorio facilitar esta información al vendedor de la licencia en la compra de la solución Enterprise Security Suite de Dr.Web. El número de Servidores Dr.Web utilizados no incrementa el precio de la licencia.

Las propiedades de la licencia, así como el uso de los archivos clave para una red antivirus ya existente, se describen detalladamente en el **Manual del administrador**, punto Administrador de licencias.

El archivo clave de licencia puede incluirse en el paquete del antivirus Enterprise Security Suite de Dr.Web durante la compra. Sin embargo, por lo general suelen suministrarse únicamente números de serie.

El archivo clave de licencia se envía a los usuarios por correo electrónico, por lo general después de registrar el número de serie en una página web especial (la dirección de la página de registro es http://products.drweb.com/register/, si no se indica una dirección distinta en la tarjeta de registro suministrada con el producto). Entre en la página web indicada, rellene el formulario con los datos del comprador e introduzca en el campo indicado el número de serie de registro (se encuentra en la tarjeta de registro). A la dirección que indique se enviarán los archivos clave. También puede descargarlos directamente de la página indicada.

Los archivos clave se envían al usuario en un archivo zip que contiene uno o varios archivos clave para las estaciones protegidas.

El usuario podrá recibir los archivos clave de una de las siguientes formas:

- por correo electrónico (generalmente después del registro en una página web, ver más arriba);
- junto con la distribución del producto si los archivos de licencia se incluyen en el paquete de la distribución del producto;
- en un soporte distinto en forma de archivo.

Se recomienda guardar el archivo clave de licencia hasta su fecha de caducidad y utilizarlo en la reinstalación o la restauración de los componentes del programa. En caso de pérdida del archivo

clave de licencia, puede repetir el procedimiento de registro en la página web indicada y recibir de nuevo el archivo clave de licencia. Para ello será necesario indicar el mismo número de serie y los mismos datos del comprador que se indicaron en el primer registro; únicamente puede cambiarse la dirección de correo electrónico. En ese caso, el archivo clave de licencia se enviará a la nueva dirección.

Para probar el antivirus se puede utilizar archivos clave de demostración. Estos archivos clave facilitan una funcionalidad total de los componentes antivirus principales, pero tienen un periodo limitado de validez. Para obtener archivos clave de demostración, es necesario rellenar un formulario ubicado en la página https://download.drweb.com/demoreq/biz/. Cada solicitud se estudia individualmente. En caso de que la solicitud sea aceptada, los archivos clave se enviarán a la dirección que haya indicado.

El uso de los archivos clave obtenidos en el proceso de instalación del programa se describe en el **Manual de instalación**, punto Instalación del Servidor Dr.Web.

Anexo B. Soporte técnico

En caso de problemas durante la instalación o en el funcionamiento de los productos de la compañía, antes de solicitar asistencia a la sección de soporte técnico se recomienda intentar encontrar una solución mediante los siguientes métodos:

- consulte las últimas versiones de las descripciones y los manuales en la dirección https://download.drweb.ru/doc/;
- lea la sección de preguntas frecuentes en la dirección http://support.drweb.ru/show_faq/;
- intente encontrar una respuesta en la base de conocimientos de Dr.Web, en la dirección http://wiki.drweb.com/;
- visite los foros de Dr.Web en la dirección http://forum.drweb.com/.

Si después de ello no ha logrado resolver el problema, puede utilizar uno de los siguientes canales para ponerse en contacto con el servicio de soporte técnico de la compañía Doctor Web:

- rellene el formulario web del apartado correspondiente en la sección http://support.drweb.com/;
- llame al número de teléfono de Moscú: +7 (495) 789-45-86 o a la línea gratuita desde toda Rusia: 8-800-333-7932.

Puede obtener información sobre las delegaciones y oficinas regionales de la compañía Doctor Web en la página web oficial http://company.drweb.com/contacts/moscow.