Dr.WEB®
since 1992

Dr.Web Enterprise Security Suite 12.0 Upgrading from versions 6.00.x and 10.0/ 11.x

Dr.Web Enterprise Security Suite 12.0

Upgrading from versions 6.00.x and 10.0/11.x

Important! Before initiating the upgrade procedure, it is recommended that you study the relevant sections of the Dr.Web Enterprise Security Suite 12 product documentation, including the **Upgrading Dr.Web Agent** section.

Contents

1. Upgrading Dr.Web Enterprise Security Suite for Windows server software

Previously installed Dr.Web Enterprise Security Suite versions 6 and 10/11 are automatically upgraded to version 12.0, and within version 12.0, by the installer. However, its configuration files are substantially different because compared with previous versions, Dr.Web Enterprise Security Suite 12 has a broader range of features.

Settings in these sections and repository settings will be reset to default. In this regard, when upgrading Dr.Web Enterprise Security Suite from version 10 and earlier versions, the settings from the following Control Center sections will not be transferred:

- The configuration **Dr.Web Server → Network → Download (download.conf)**;
- Dr.Web Server remote access (frontdoor.conf);
- Web-server configuration (webmin.conf).

  In addition, user routines that have been set up manually will not be available after the upgrade. If you want to keep your settings from earlier versions, specify them manually after the Dr.Web ESS server is upgraded, using your configuration backups stored in the directory selected for backups during the installer-facilitated upgrade process:

- when upgrading from version 6: <installation_disk>:\DrWeb Backup;
- when upgrading from versions 10, 11 and within version 12: specify **Back up Dr.Web Server critical data during the upgrade** (by default <installation_disk>:\DrWeb Backup).

  The list of stored files is available in the documentation.

Important!

- Beginning with server version Dr.Web 10, the MS SQL CE database is no longer supported. When the server is being upgraded by the installer, the MS SQL CE database is automatically converted into an embedded SQLite database;
- If an anti-virus network has workstations/servers running Windows XP/Windows Server 2003 (64-bit versions), the given stations must be transferred to a separate network running Dr.Web Enterprise Server version 6 because it is impossible to upgrade them;
- Due to differences in version features, after the upgrade you must carefully check the settings of all groups and stations to ensure they comply with established security policies and adjust them, if necessary;
- For an anti-virus network that uses the Dr.Web Proxy Server, you must also upgrade the Proxy Server to version 12.0 when upgrading the components to version 12.0. Otherwise, it will be impossible to connect the Agents delivered with version 12.0 to the Dr.Web ESS server. It is recommended that you upgrade in the following order: Dr.Web Server   Dr.Web Proxy Server   Dr.Web Agent;

  When upgrading Dr.Web ESS server from version 6 to version 12, the Dr.Web ESS server settings will not be stored via the proxy server. After installing version 12, you must manually specify the connection settings via the proxy server (see the Administrator Manual's "Proxy" section);

- When upgrading Dr.Web ESS server to version 12, the upgrades of the repository products Dr.Web Agent for Android, Dr.Web Agent for UNIX, and Dr.Web Proxy Server are downloaded from the GUS by default only when these products are requested from the stations. For more information refer to the Administrator Manual's "Detailed repository configuration" section;
- If Dr.Web ESS server is not connected to the Internet and upgrades are downloaded from another server or via the Repository downloader, before installing or upgrading the products

for which the **Upgrade on demand only** option is enabled, you must first manually download these products to the repository.

Important! Before initiating the upgrade procedure, it is recommended that you:

- Create a server backup containing files important for you (for example, report templates that are in the directory \var\templates) and save it in a directory that does not contain Dr.Web Enterprise Security Suite;

- Verify the TCP/IP settings in order to connect to the Internet. In particular, the enabled DNS service should have the proper settings;

- Manually remove the additional distribution of Dr.Web Enterprise Security Suite (extra), if it had been installed previously.
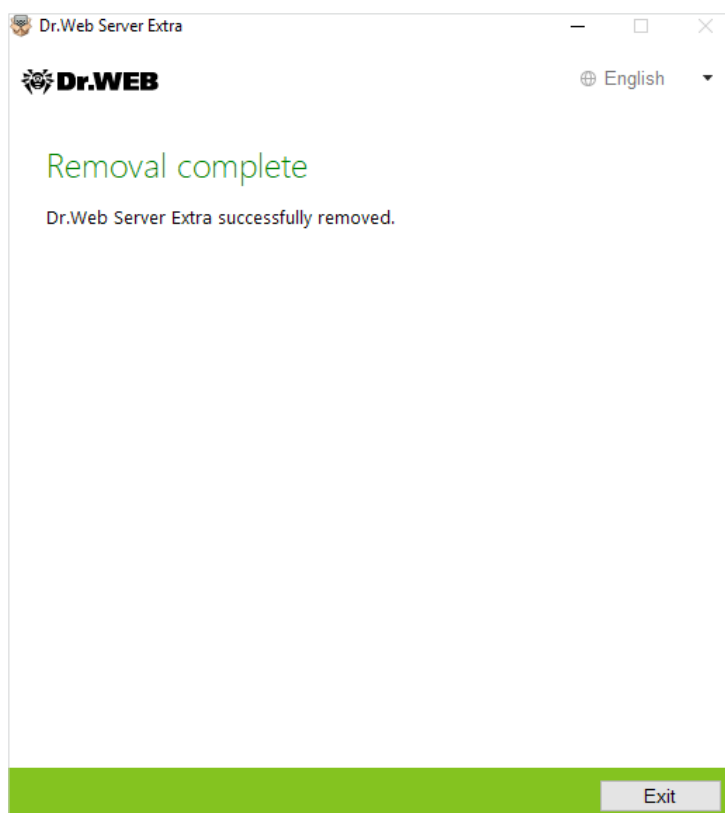
   To remove this distribution, open **Control Panel → Programs and Features**.
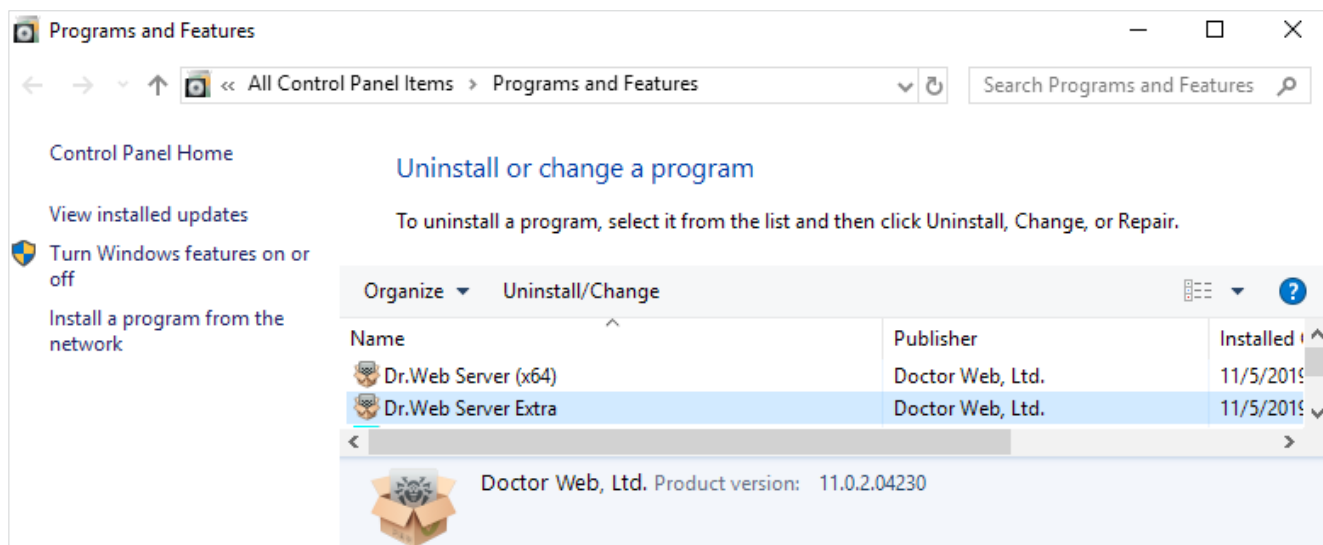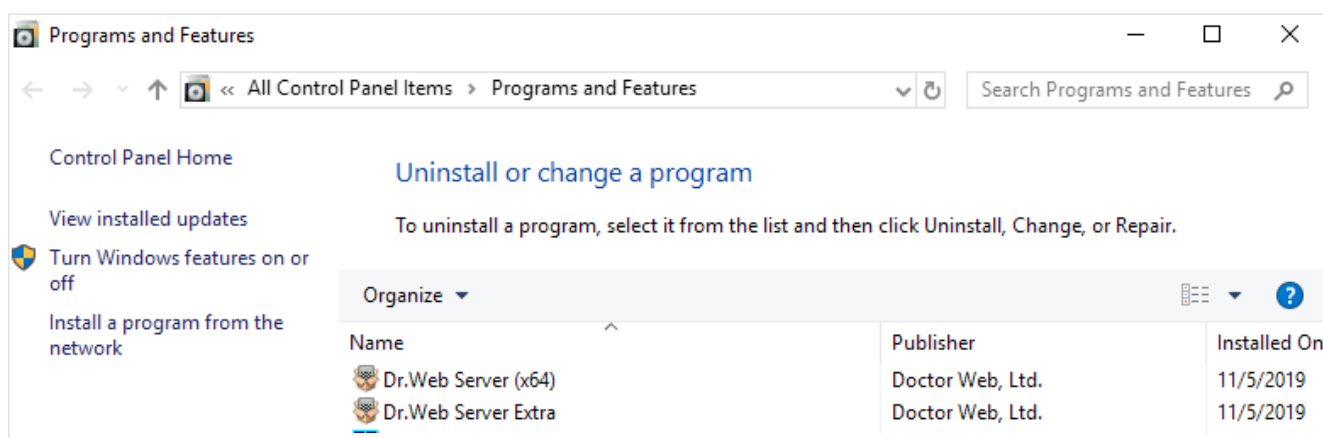
In the newly opened window, select the Dr.Web ESuite Extra distribution you need to remove, and click on **Remove**.
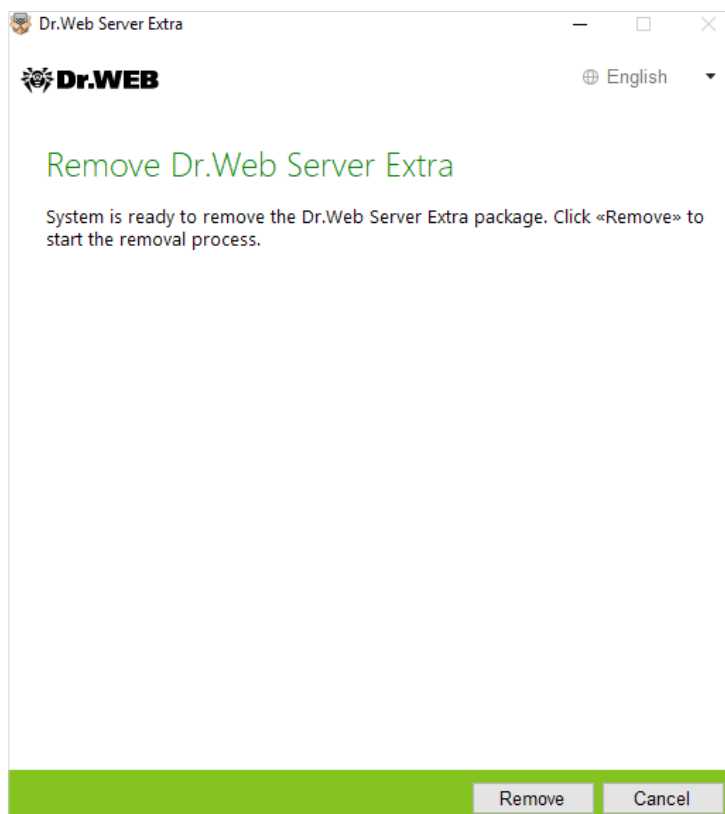
The removal procedure is straightforward and is performed automatically.

- Back up the database. Without a database backup, you will not be able to restore the anti-virus server in the event of unforeseen circumstances.

Important! During the installation process, the embedded database is upgraded, and the configuration file of the Dr.Web administration server is converted by the installer.

These files cannot be replaced by automatically saved copies when upgrading from version 6. Before you start the backup, install the anti-virus server. You can do this using the Dr.Web Control Center command or by selecting **Start**, then **Dr.Web Server → Stop** .
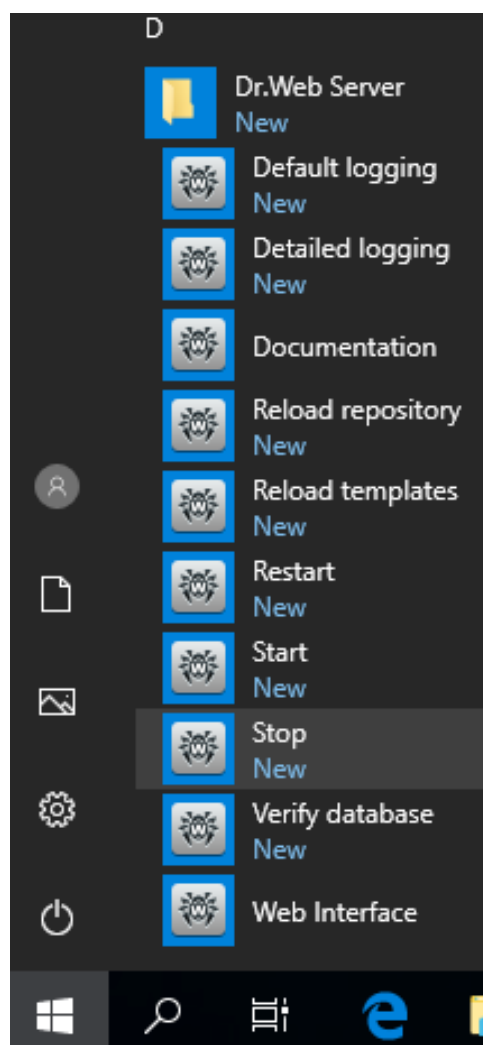

Use the Task Manager to make sure that all the processes with the drwcsd.exe name are missing in the memory.

The following dialogue indicates that the server has stopped:
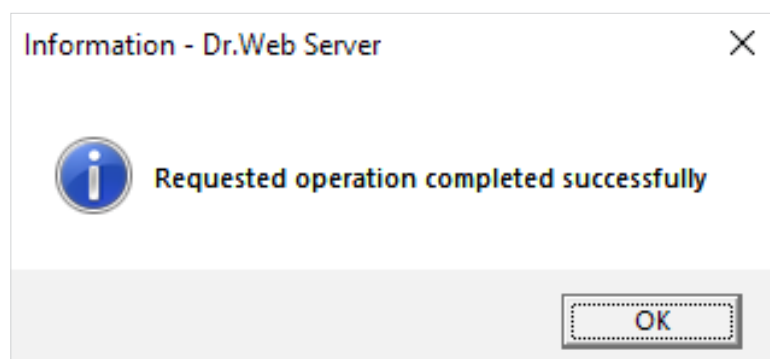
Go to **Start — Dr.Web Server**, select **Check database** and wait for the message showing the result of the selected action.

If you receive a message informing you that the verification was successful, close it and move to the next step.
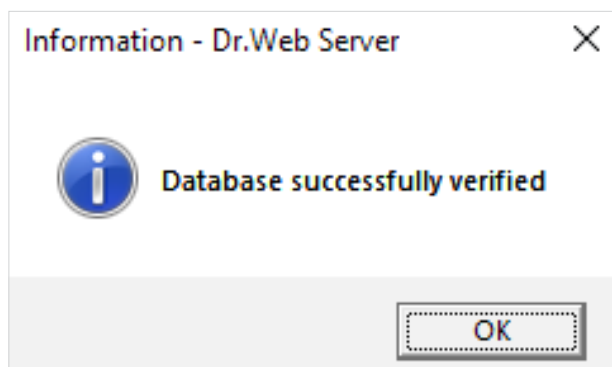
The internal database is exported into a file using the following command in the command line Cmd:

```
"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 <
backup_directory >\esbase.es
```

for example, for Dr.Web server version 6

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise
Server\var" -verbosity=all exportdb c:\temp\esbase.es
```

If you are using an external database, it is recommended that you use the standard tools supplied with the database.

Note. Instead of C:\ drive, you can specify any other convenient location where there is enough free space. This command exports the contents of the Dr.Web ES server database into the esbase. es file on drive C:\.

Important! The installation directories of 32-bit and 64-bit versions of the anti-virus server differ. So, if you install the 32-bit version of Dr.Web Enterprise Security Suite on the 64-bit version of MS Windows, the command will be as follows:

```
"C:\Program Files (x86)\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files
(x86)\DrWeb Server" -var-root="C:\Program Files (x86)\DrWeb Server\var"
-verbosity=all exportdb C:\temp\esbase.es
```
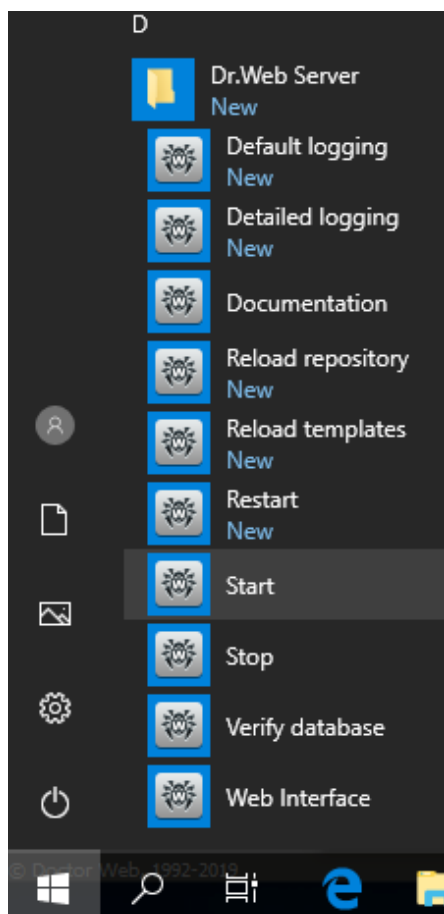
Make sure that Dr.Web Enterprise Security Suite database was exported successfully.

Without a database backup, you will not be able to restore the Dr.Web ESS server software in the event of unforeseen circumstances.
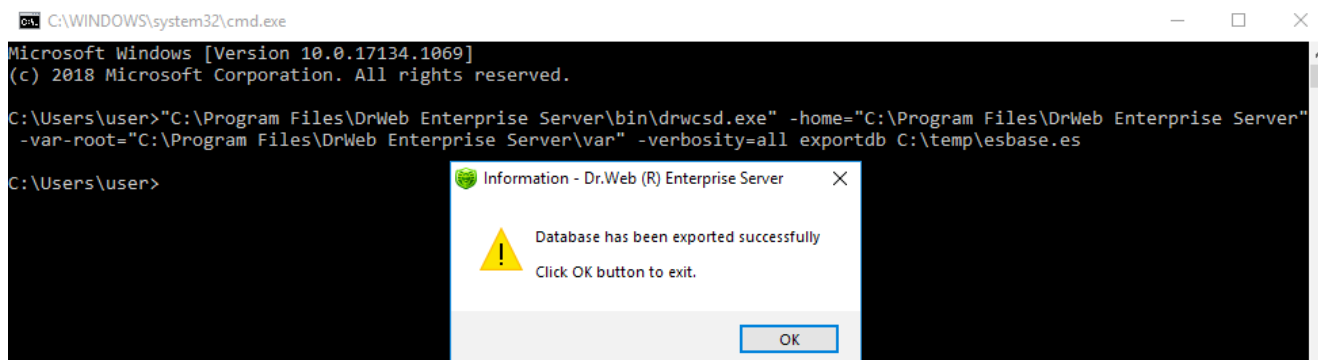
When the export process is complete, start the server using the command from the menu **Start — Dr.Web Server — Start**.

▪ Due to the fact that inter-server upgrades are not transmitted and the inter-server connection is used only to transmit statistics between Dr.Web administration server versions 12 and 6, it is recommended that you disrupt the hierarchical connections between servers in advance and restore them after the upgrade procedure completes successfully **on all** the servers included in the general hierarchical network for transmitting inter-server upgrades.

Also, the disruption of inter-server connections is recommended because when upgrading to version 12, information about unsupported repository items may be transmitted between Server versions 10 and 12. The items may include legacy products that are not available in the new Dr.Web ESS server's repositories as well as new products that are not present in the old Server's repository. As a consequence, unknown repository products can cause upgrading errors. The "Repository Content" section will only display the location directories for such products, instead of names.

To removal a hierarchical connection, do the following:

▪ In the Control Center's main menu, select **Neighbourhood**.

▪ In the newly appeared window that contains the hierarchical list of anti-virus network servers, select the parent server, and then click on **Delete**. Then confirm the operation.

If there are other servers with which inter-server communication is set, repeat the operation with them.

If there are child servers, it is recommended that you compile them in a list and then upgrade them and restore the inter-server communication with them in accordance with the documentation.

Restore the hierarchical connections after all the Dr.Web administration servers are updated.

If you want to leave Dr.Web administration servers of earlier versions in your Dr.Web anti-virus network to connect Agents installed on operating systems that are not supported by version 12, the Dr.Web administration server version 6 and version 12 should receive the upgrades independently. To ensure the transfer of inter-server upgrades, upgrade all the Dr.Web ESS servers.

1.1. Upgrading Dr.Web Enterprise Security Suite 6 for Windows server software

Important! The Dr.Web server license key is no longer used for versions 10/11/12. If you are going to use the configuration files from Dr.Web ESS server version 6, note that the embedded database is upgraded, and the Dr.Web ESS server configuration file is converted by the installer. These files cannot be replaced with automatically saved copies when switching from Dr.Web ESS server version 6.

Due to the fact that the upgrade procedure is different for different versions, if your organisation uses Dr.Web 6.00.0 and 6.00.4 server versions, before upgrading, determine the current Dr.Web server version installed at the moment. To do this:

1. in the server management interface, select the **Administration** tab;
2. check the information in the top row next to **Dr.Web Enterprise Server version** (see example).
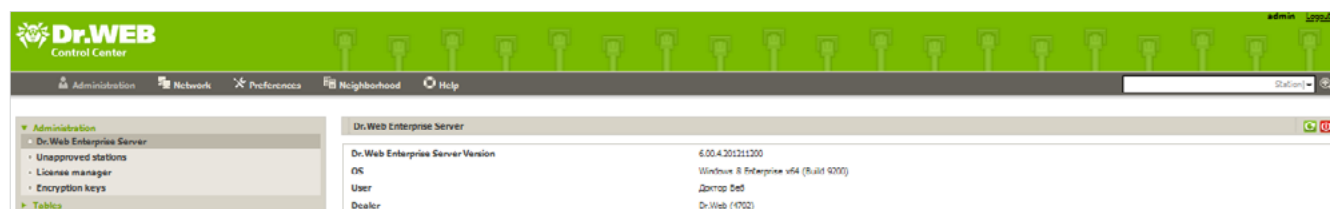
In order to ensure that your corporate anti-virus protection remains uninterrupted, below we will discuss how to perform an upgrade using two servers — with the agents transferred to the second server during the upgrade procedure.

Run the utility to be used with the drwidbsh internal database on the server on which the new Dr.Web server is deployed (hereinafter — Machine № 2) with the same or similar characteristics (hardware / operating system / network connections with the same access permissions) as the server on which Dr.Web server version 6 was previously deployed (hereinafter — Machine № 1). To do this, enter the following in the Cmd command line:

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwidbsh.exe" "C:\Program Files\
DrWeb Enterprise Server\var\dbinternal.dbs"
```

In the window of the running drwidbsh utility, enter the following three commands:

```
1. pragma integrity_check;
```


The command additionally checks the database.

```
2.delete from procerror;
```

> With this command, you can clear the error table, which is not necessary for subsequent migration to version 10 and can occupy a large amount of memory.

```
3.vacuum;
```

> With this command, you can remove unused pieces from the database files, reducing the size of the file on the disk.

You can access the database only if Dr.Web server is installed.

Note. The semicolon at the end of each command is required.

The command execution can take from a few minutes to a few hours. The process is highly dependent on the file system capacity, the degree of its fragmentation, and how loaded the subsystem disk is with other tasks.

If the command is completed without errors, exit the drwidbsh program to Cmd and proceed to the next step.

Copy the following files to the random empty directory of Machine № 2 from the server on which the Dr.Web Control Center was previously installed:

- C:\Program Files\DrWeb Enterprise Server\etc\drwcsd.pri;

  - files of the server database in use, for example, C:\temp\esbase.es — if you are using an embedded database;

  - enterprise.key and agent.key. These key files of your active license can be exported from the administration server web interface (the **License Manager** section), copied from the folder C:\Program Files\DrWeb Enterprise Server\etc, or saved from the email message to which they were sent when the serial number was registered.

Install Dr.Web anti-virus server on Machine № 2. When installing Dr.Web server version 6.00.4 ES on Machine № 2, specify the installer settings:

- the use of existing cryptographic keys (file drwcsd.pri);
- license keys (enterprise.key and agent.key);
- the creation of a new database using the internal IntDB database (by selecting the appropriate steps in the installation wizard).

Leave all the other installation parameters as whatever the installer prompts by default.

After the installation, connect to the Dr.Web Control Center installed with the new Dr.Web server version 6.00.4 on Machine № 2, and make sure it works properly and updates its repository. To do this:

1. Go to the **Administration** section.

2. On the left side of the screen, select **Repository state** in the **Configuration** section.

For a simple check, it is enough to look at **Last revision since** section and make sure that the dates of the virus databases are relevant (current day-month-year). If the dates are wrong, click on the **Check for updates** button.

Stop the Dr.Web server using the command from the Control Center or the menu command **Start — All programs — Dr.Web Enterprise Server — Server management — Stop**.

Run the drwcsd.exe file with the importdb key to import the database contents from the esbase. es file. To do this, type the following command in the Cmd command line:

```
"C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise
Server\var" -verbosity=all importdb "C:\esbase.es"
```

You can access the database only if the Dr.Web server is stopped.

The directory with:\esbase.es is specified as an example; you should use the location to which you previously copied the database files.

If you use a different database, use the standard utilities to work with your database.

After the import process has completed, check the database using the command **Start — All programs — Dr.Web Enterprise Server — Server management — Stop — Verify database**. Wait for the notification containing the scan results.

Start Dr.Web ES server on Machine № 2 with the command from **Start — All programs — Dr.Web Enterprise Server — Server management — Launch**. Connect to its Control Center.
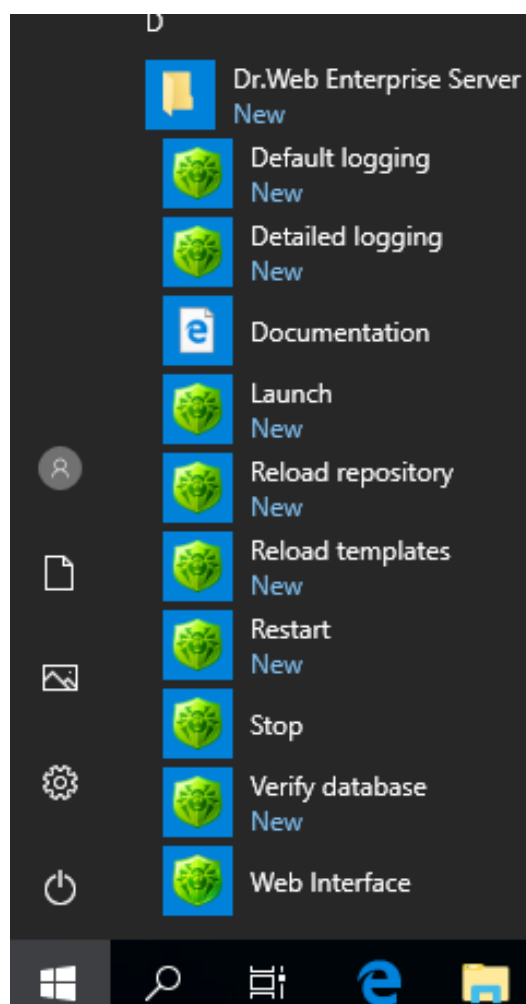
Make sure the station's status is shown as offline in the anti-virus network list. If this condition is satisfied, stop the Server from the Control Center or with the command **Start — All programs — Dr.Web Enterprise Server — Server management — Stop**, and go to the next step in the instructions.

If some stations are displayed with the online status, create a support request.

Make a backup of the C:\Program Files\DrWeb Enterprise Server directory in a safe storage location.

In the Machine №2 Control Center, make sure that its repository upgrades correctly (the repository status should display the current dates of the anti-virus database upgrades).

If you are upgrading from Dr.Web ES 6.00.0, in the **Administration** section, open **Dr.Web Server** and make sure the version date coincides with the date in the repository that was verified in the previous step. If the dates are the same, go to the next step. If you see a different version or date, take a screenshot and attach it to the comment in your support request and stop on this step.

Once you make sure that the new server is working properly (see the previous two steps), you can shift to transferring the agents from the old Dr.Web ES server to the new one. It's better to transfer the agents separately or in small groups. If, during the upgrade process, machines are encountering problems, stop switching other computers to the new server and contact the Doctor Web technical support service.

To transfer stations to the Machine № 1 Control Center, select the station or the group of stations that you are going to transfer to the Machine № 2 Dr.Web server. Open the agent settings and select:

- the **Anti-virus Network** section,
- a group or a station from the list,
- **Configuration** on the left of the screen,
- **Dr.Web Enterprise Agent for Windows**.

In the **Network** tab, enter the network address of the new server in the **Server** field (Machine № 2) and save the settings.
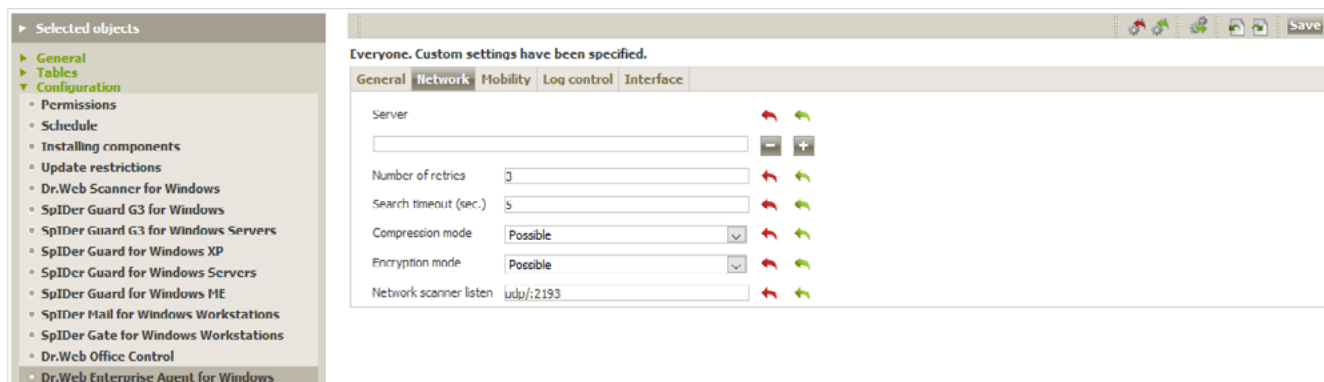
Note. During the upgrade process, the components of the earlier version are first completely removed, including the interface module, in which case the anti-virus could fail to inform you about the need to do an initial system restart. If a restart was not requested, you should restart the computer with the upgraded agent manually 2 – 3 minutes after the agent icon disappears from the system tray. Do not postpone the restart since a station remains unprotected after the agent's removal.

If you are using Dr.Web Enterprise Security Suite 6.00.0, after transferring all the agents to the new Machine № 2 server, you must upgrade the old Machine № 1 server by running the distribution version 6.00.4 and following the installation wizard's instructions. If an error occurs during the upgrade process, you should create a request for the technical support service). After this, you can upgrade server version 6.00.4 to version 12.

To upgrade the administration server on Machine № 1, you should download the 32-bit or 64-bit version of the distribution in the Download Wizard section of www.drweb.com.

Run the distribution file. A window will open, notifying you that a previous version of the server software is present and providing you with a brief description of the procedure for upgrading to the new version. To start configuring the upgrade process, click on **Upgrade**.


The default installer's language is the language of the operating system. If necessary, you can change the language at any step by selecting the appropriate option in the top-right corner of the installer window.

If the computer on which you install the Dr.Web server is already running Dr.Web Agent with active Dr.Web self-protection, a corresponding notification will be displayed. Use the Agent settings to disable this module and click on **OK** to continue the installation or on **Cancel** — to abort.

A window with information about the product and a link to the license agreement will appear. After reading the license agreement, select **I accept the terms of License agreement** to continue with the upgrade and click on **Next**.
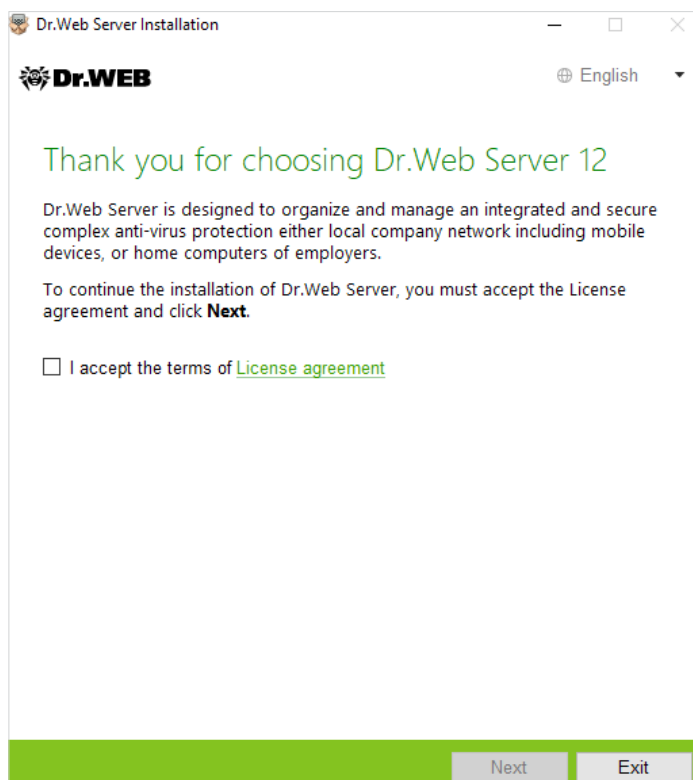
In the subsequent steps, the server will be configured the same way the Dr.Web server is installed, using the configuration files of the previous version.
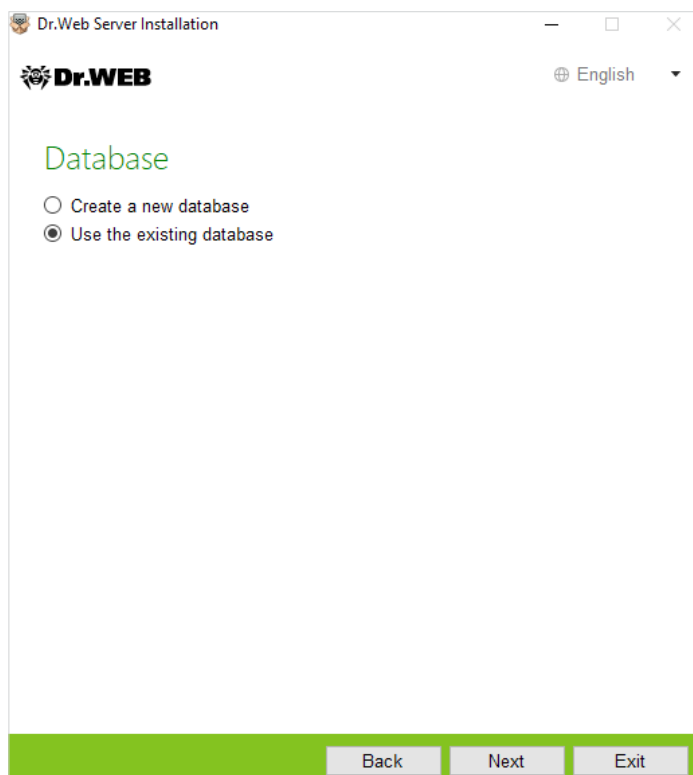
The upgrade will be performed automatically using the previously saved backups containing the information you need.

The installer automatically detects the Dr.Web ESS server installation directory, the location of the configuration files, and the embedded database of the previous installation. If necessary, you can change the file paths automatically found by the installer.
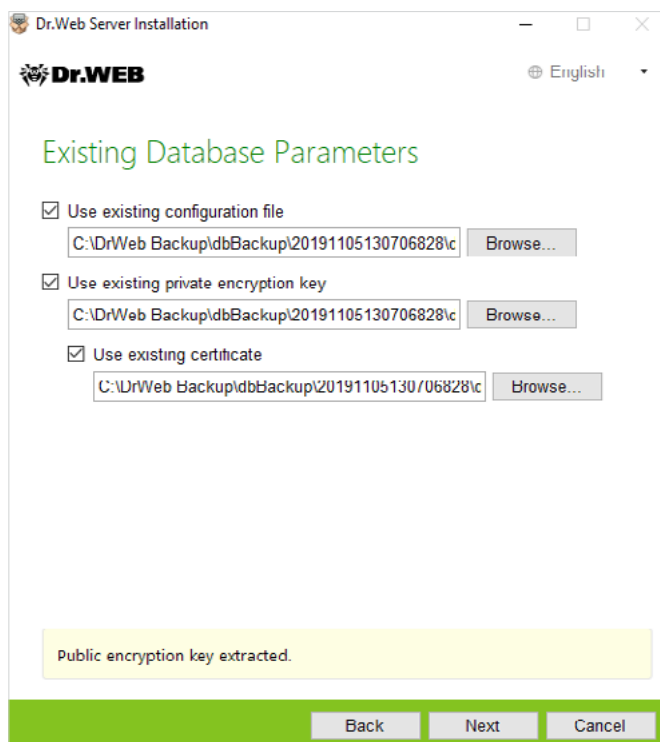
When using an external server database during the upgrade, select **Use existing database**.

If you plan to use an Oracle or a PostgreSQL database as an external database via an ODBC connection, when upgrading the server, in the installer settings, cancel the installation for the appropriate database (in database support data).

Otherwise, you will not be able to use Oracle via ODBC because of a library conflict.
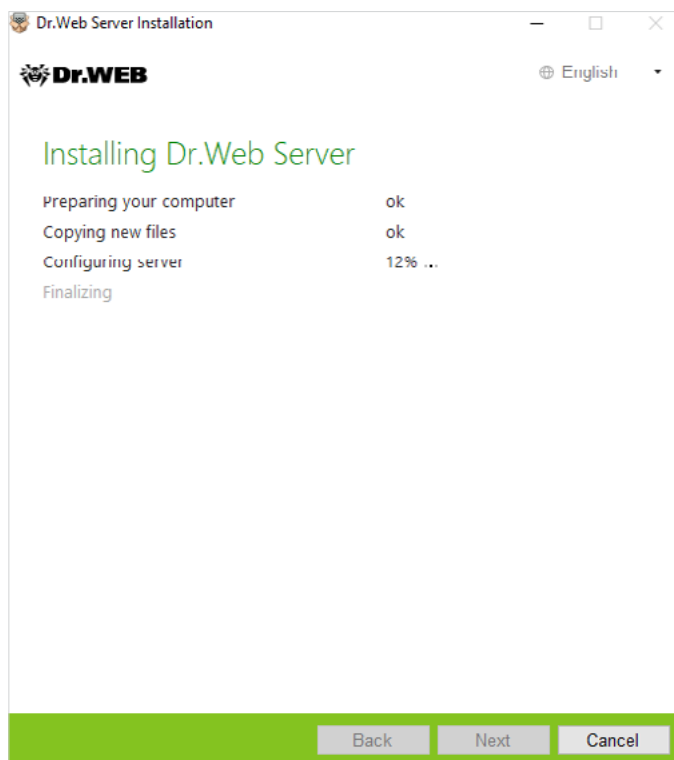

Before the installation, check the server parameter configuration by clicking on **Additional parameters**.
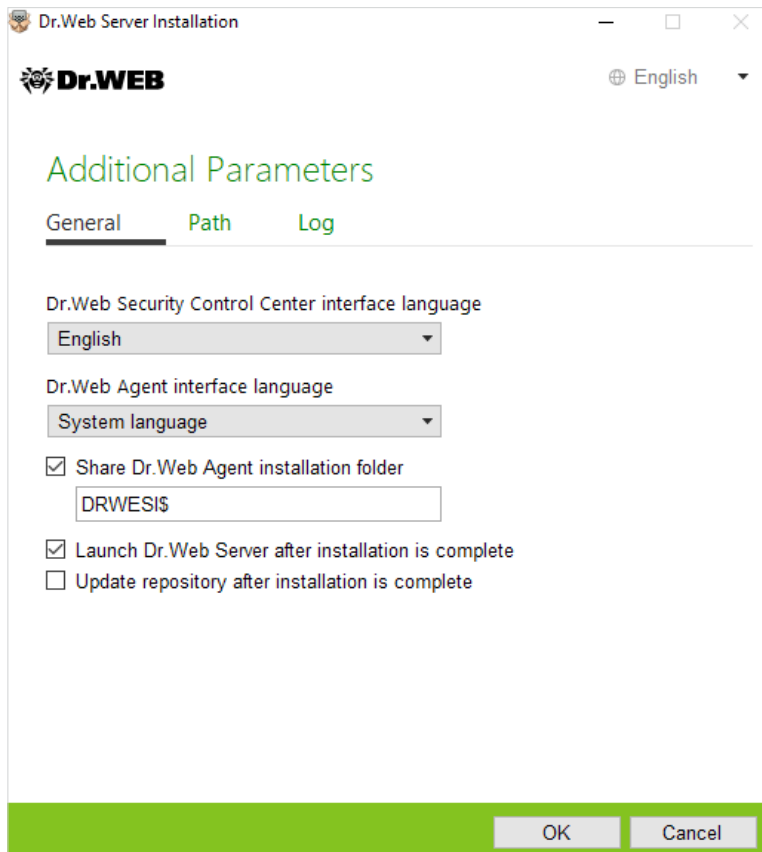
To start removing the previous server version and installing server version 12, click on **Install**.

Note. After upgrading your anti-virus network's Dr.Web ESS servers, you must reconfigure the encryption and compression settings for the linked servers (see the Administrator Manual's **Configuring connections between Dr.Web Servers** section).

Once the Dr.Web server has been upgraded, clean the browser cache used to connect to the Control Center.

Important! In version 12, the Dr.Web Control Center extension has been discontinued. The corresponding distribution can be removed from client workstations. After the Machine № 1 server has been upgraded to version 12.0, you must check to see whether it is operational. For example, check the virus databases in the appropriate section of the Control Center the same way as was done previously.

It should be noted that the interface of the required sections in version 12 has been revamped:
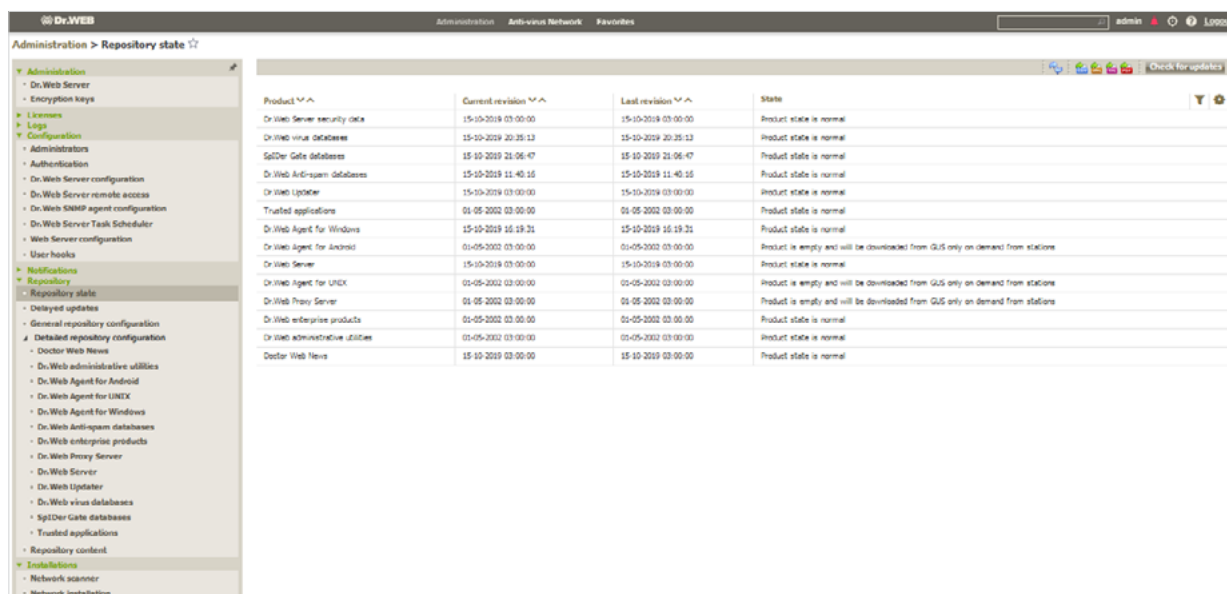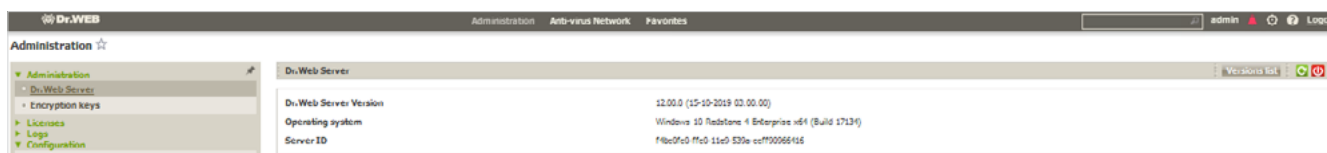
After finishing your check, you should switch all the agents back to it. Once you have switched the agents, the intermediate server version 6.00.4 can be removed.
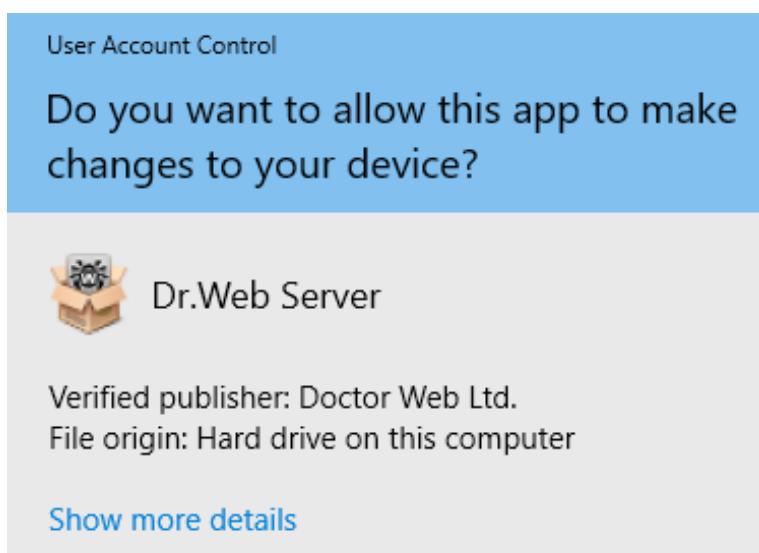
If you have any questions or encounter any problems during any of these steps, contact Doctor Web's technical support service.

1.2. Upgrading Dr.Web Enterprise Security Suite 10/11 for Windows server software

To upgrade Dr.Web Enterprise Security Suite from version 10/11, run the actual distribution file and, if necessary, confirm its launch.

The upgrade procedure may differ slightly from the upgrade procedure from version 10 .0 and version 10.0.1, 10.1, and 11, and within version 12.

The bit version of the distribution should coincide with the bit version of the installed version.

The default installer's language is the language of the operating system. If necessary, you can change the language at any step by selecting the appropriate option in the top-right corner of the installer window.

If the bit version is the same, a window will open, notifying you that a previous version of the server software is present and providing you with a brief description of the procedure for upgrading to the new version.

To start configuring the upgrade process, click on **Upgrade**.

In the newly opened window, select **I accept the terms of the License agreement** after first reading it. Click on **Next** to continue.

To start removing the previous server version and installing server version 12, click on **Install**.

In the newly opened window, the installer prompts you to save the configuration files of the upgraded version. You can select a directory other than the default directory used for backups.

Important! It is recommended that you tick the **Back up Dr.Web Server critical data** box.

When upgrading Dr.Web ESS server from versions 10/11, and within version 12, using the installer, the configuration files are stored in the directory specified in **Back up Dr.Web Server critical data** during the upgrade process (by default <installation_disk>:\DrWeb Backup).

If you do not want to do a backup, clear the **Back up Dr.Web Server critical data** box.

Click on **Uninstall** to continue.
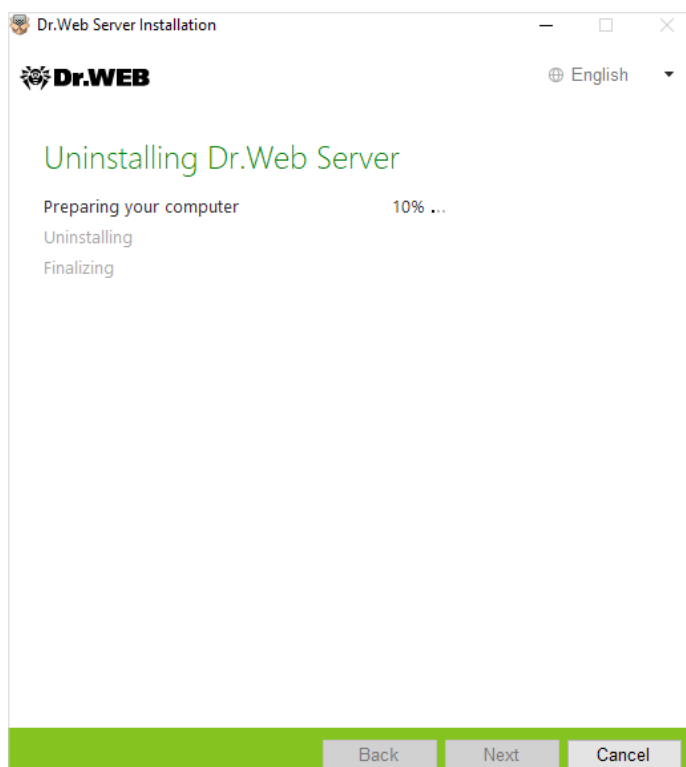
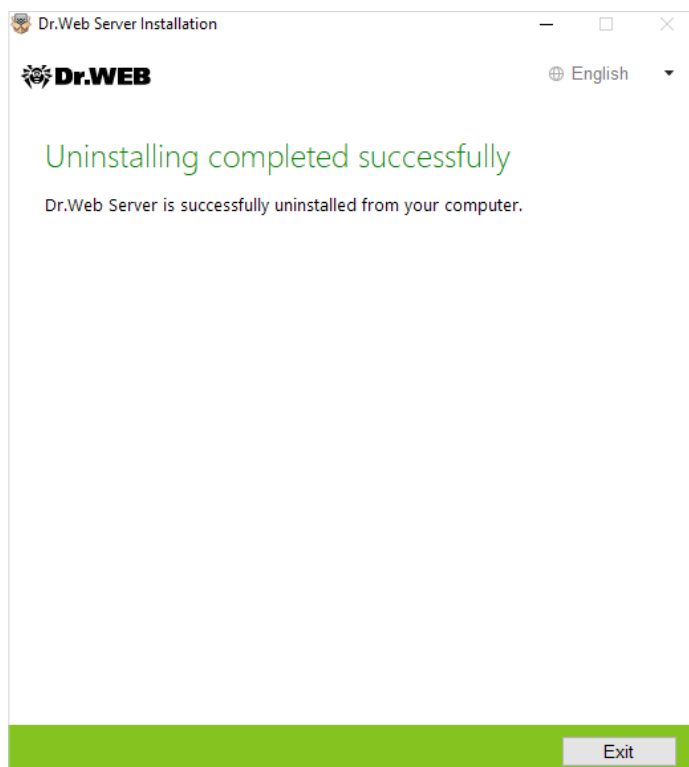Once the installed server has been removed, the steps performed in the installation wizard do not differ from those performed during a typical product installation.
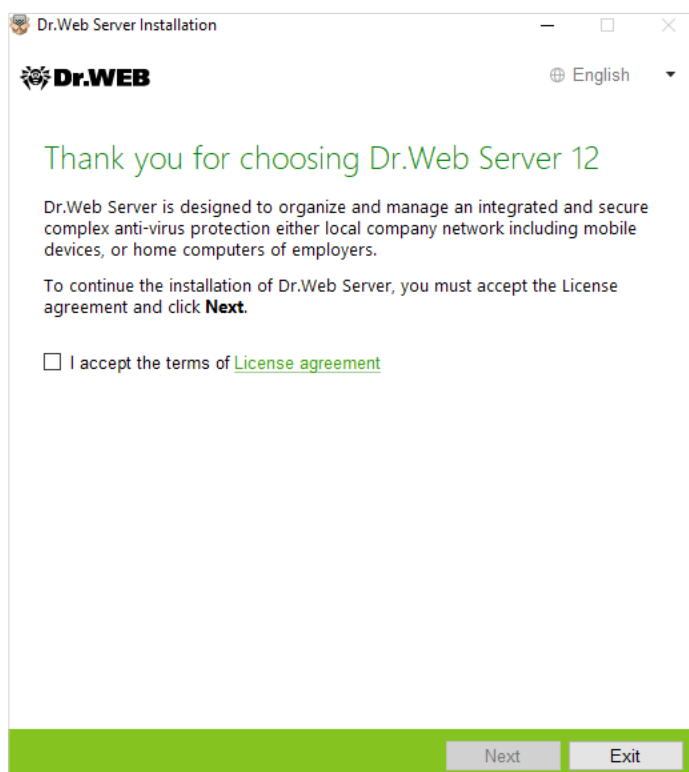
When using an external server database during the upgrade process, select **Use existing database**.

If you plan to use an Oracle or a PostgreSQL database as an external database via an ODBC connection, when installing (upgrading) the Dr.Web ESS server, in the installer settings, cancel

the installation of the integrated Oracle client (**Oracle database driver** in the **Database support** section). Otherwise, you will not be able to use Oracle via ODBC because of a library conflict.
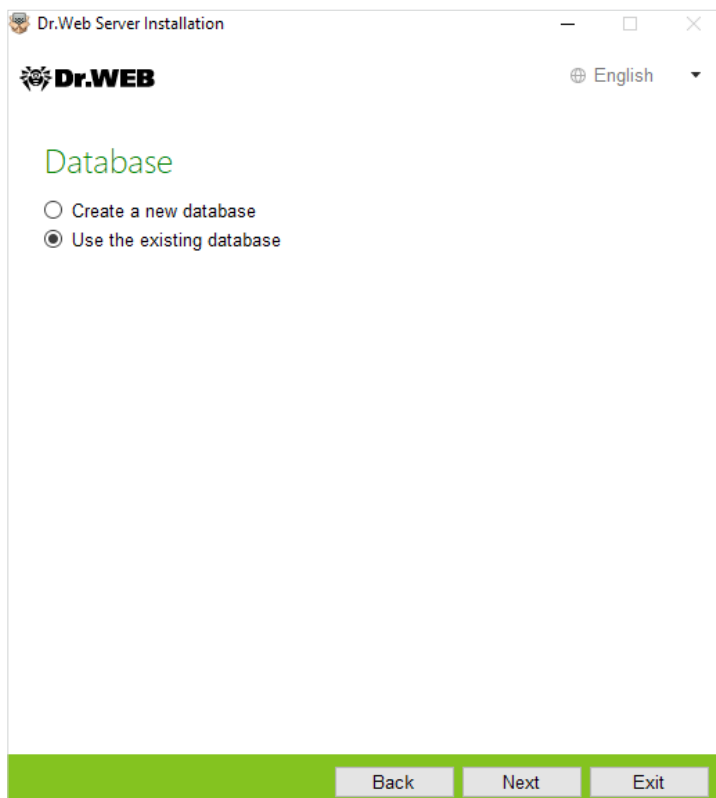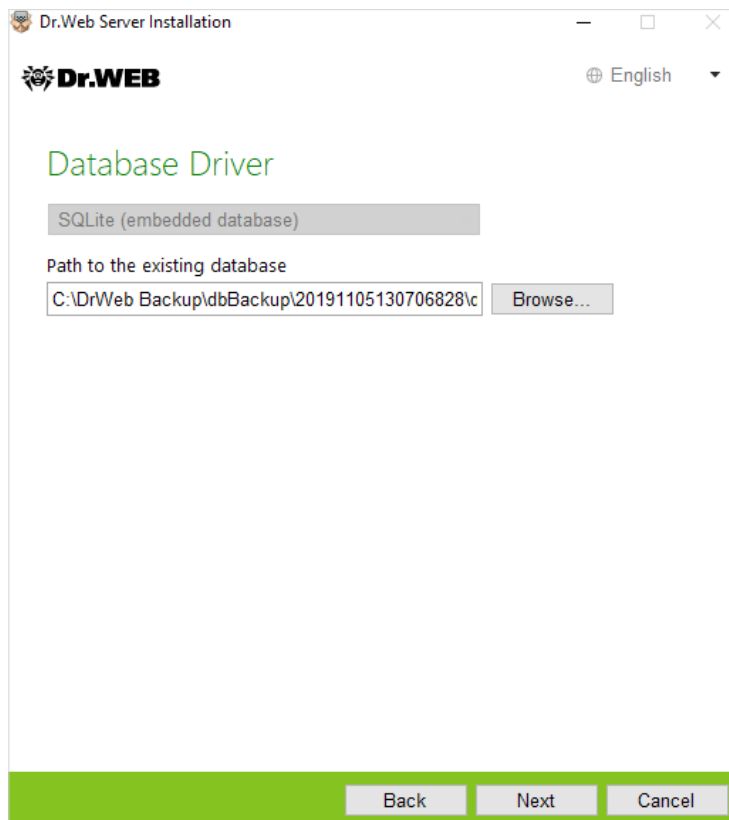
If you are using an existing database, you can configure the parameters of the database you are using.
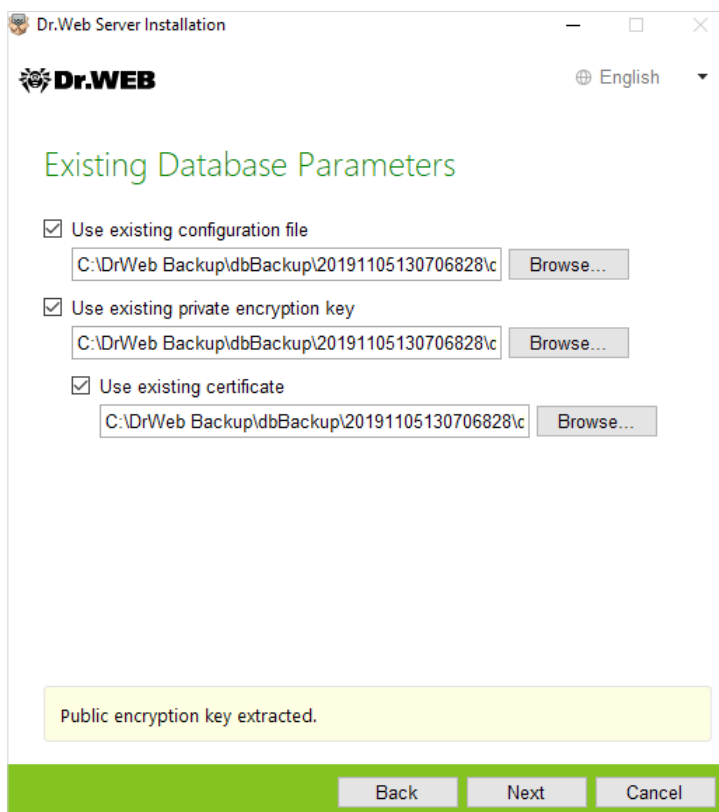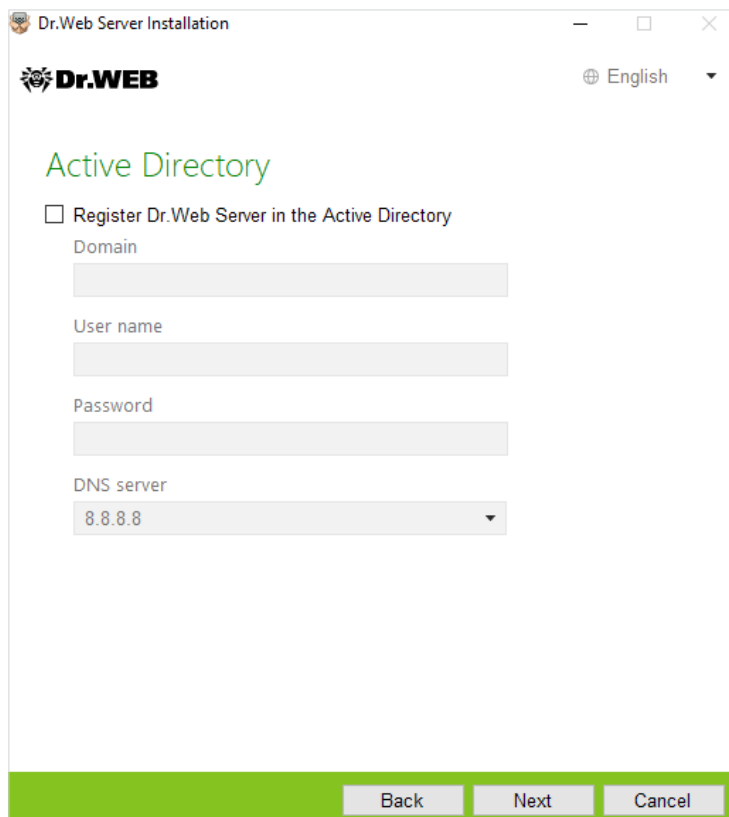
The drwcsd.conf file should be specified as the configuration file.

Important! When upgrading a Dr.Web Enterprise Security Suite server to the new version, you are not required to select **Use existing certificate** and specify a certificate in this window.
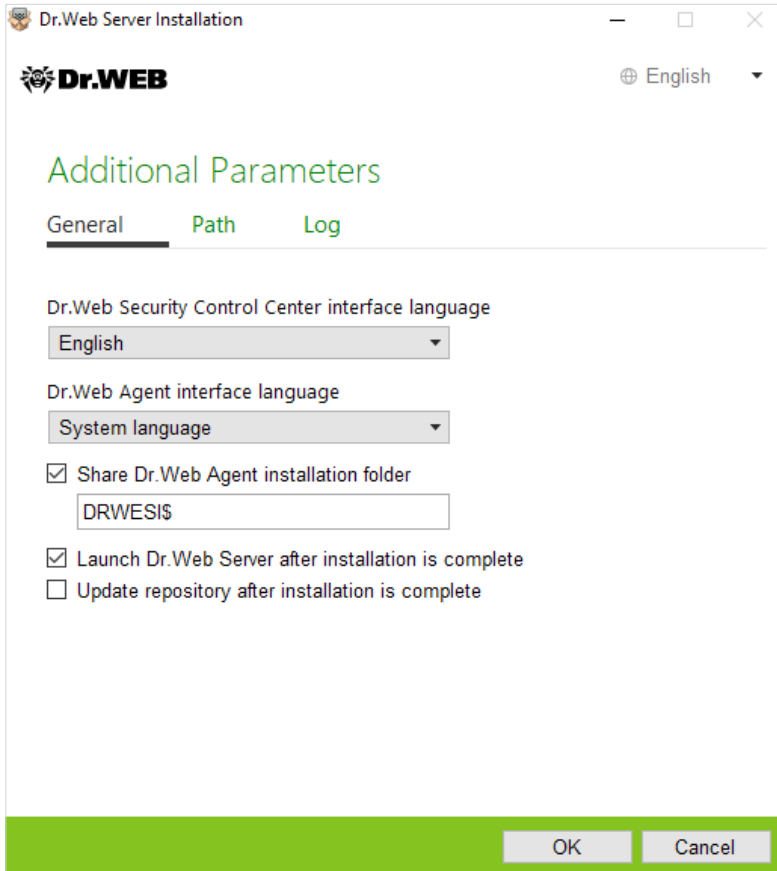
In the **Path to the existing database** field, you should specify the path to the stored database backup copy. For example, a file with the *.gz or *.sqlite extension.

In the additional parameters window, you can indicate the components that do not need to be installed.

Dr.Web Server Installation

⊕ English ▼

Installing Dr.Web Server

Preparing your computer	31% ...
Copying new files	
Configuring server	
Finalizing	

Back   Next   Cancel

Dr.Web Server Installation

⊕ English ▼

Installation completed successfully

Dr.Web Server is successfully installed on your computer.

Open Anti-virus Network Quick Installation Guide

Exit

2. Upgrading Dr.Web Enterprise Security Suite 6/10/11 for UNIX server software

Dr.Web Enterprise Security Suite 12 incorporates more features than previous versions which is why its configuration file settings are substantially different.

In this regard, when upgrading Dr.Web Enterprise Security Suite from version 10 and earlier versions for the UNIX family of operating systems, the settings from the following Control Center sections will not be transferred to version 12.0:

▪ web-server configuration (the webmin.conf file).

The settings in these sections will be reset to default. During the upgrade process facilitated by the installer, the configuration files of the upgraded version are stored in the directory selected for backups. The list of stored files is available in the documentation.

The procedure for upgrading from version 6.0.4 to version 12 needs to be performed manually. Automatic updating from versions 10/11 to version 12 of Dr.Web ESS server for identical types of packages, with the help of the installer, over the installed version is not supported for all Unix family operating systems. That's why for Unix family operating systems in which automatic upgrades cannot be performed on top of a previously installed package, upgrades must be performed manually.

You can upgrade from versions 11.x to version 12.0 via the Control Center. The description of the upgrade procedure is given in the Administrator Manual's "Upgrading Dr.Web server and restoring from backup" section.

If it is impossible to upgrade version 6.0.4 and earlier versions on top of a previously installed package, you must uninstall the earlier versions of the software, having created a backup, and use the backup to install version 12.

During the removal process and when the server is being automatically upgraded to version 12, the configuration files are saved to the default backup directory: /var/tmp/drwcs.

If you want to keep your settings from the earlier version, you will need to use your configuration backups to specify the parameters manually in the corresponding Control Center sections after the Server is upgraded.

Important! All installation steps must be performed under the **root** account.

Before upgrading Dr.Web Enterprise Security Suite, we recommend that you back up the database.

To back up the database:

1. Stop the anti-virus server:

▪ For FreeBSD:

    # /usr/local/etc/rc.d/drwcsd.sh stop

▪ For Linux:

    # /etc/init.d/drwcsd stop

2. Export the database to the file:

▪ For FreeBSD:

    # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/esbase.es

▪ For Linux:

    # /etc/init.d/drwcsd exportdb /var/opt/drwcs/esbase.es

If you are using an external database, it is recommended that you use the standard tools supplied with the database.

If you are using an external PostgreSQL database, it is recommended that you use standard PostgreSQL tools:

```
# /etc/init.d/drwcsd stop
# pg_dump -E UTF-8 -F -t -U postgres -f /root/avdesk_backup/current.dump drwcs_db
```

The user on behalf of whom the database connection is made (the -U option) and the path to the dumps may vary depending on the operating system.

Make sure that the Dr.Web Enterprise Security Suite database was exported successfully. Without a database backup copy, you will not be able to restore the Dr.Web ESS server software in the event of unforeseen circumstances.

If you want to use any of the files in the future (other than files that will be saved automatically during server removal), back up these files manually (for example, copies of report templates, etc.).

When you upgrade from versions 10/11 to version 12.0 (except for servers running **Linux** from the packages *.rpm.run and *.deb.run), the packages can be upgraded automatically. To do this, run the installation of the corresponding Dr.Web ESS server package.

During the upgrade process, the configuration files will be automatically converted and located in the required directories. Additionally, some configuration files are stored in the backup directory.

```
Do you agree with the terms of this license? (yes/NO) yes
yes
Package installation started, please wait...
=== Backing up additional configs.
Backup "/var/opt/drwcs/etc/auth-ldap.xml" --> "/tmp/tmp.Nth18dgG7N/auth-ldap.xml"
Backup "/var/opt/drwcs/etc/auth-radius.xml" --> "/tmp/tmp.Nth18dgG7N/auth-radius.xml"
Backup "/var/opt/drwcs/etc/auth-ads.xml" --> "/tmp/tmp.Nth18dgG7N/auth-ads.xml"
=== Removing the ES currently installed.
===> Removing (preun): Dr.Web(R) Enterprise Suite
===> Stopping Dr.Web(R) Enterprise Server

Please enter path to directory, in which we will pub backup: [/var/tmp/drwcs] :
===> Backup sensitive data
===> Backup: "/var/opt/drwcs/dbinternal.dbs" --> "/var/tmp/drwcs/dbinternal.dbs"
===> Backup: "/var/opt/drwcs/etc/drwcsd.conf" --> "/var/tmp/drwcs/drwcsd.conf"
===> Backup: "/var/opt/drwcs/etc/webmin.conf" --> "/var/tmp/drwcs/webmin.conf"
===> Backup: "/var/opt/drwcs/etc/drwcsd.pri" --> "/var/tmp/drwcs/drwcsd.pri"
===> Backup: "/opt/drwcs/Installer/drwcsd.pub" --> "/var/tmp/drwcs/drwcsd.pub"
===> Backup: "/var/opt/drwcs/etc/enterprise.key" --> "/var/tmp/drwcs/enterprise.key"
===> Backup: "/var/opt/drwcs/etc/agent.key" --> "/var/tmp/drwcs/agent.key"
===> Backup: "/var/opt/drwcs/etc/certificate.pem" --> "/var/tmp/drwcs/certificate.pem"
===> Backup: "/var/opt/drwcs/etc/private-key.pem" --> "/var/tmp/drwcs/private-key.pem"
===> Backup: "/var/opt/drwcs/etc/common.conf" --> "/var/tmp/drwcs/common.conf"
warning: /var/opt/drwcs/etc/webmin.conf saved as /var/opt/drwcs/etc/webmin.conf.rpmsave
warning: /var/opt/drwcs/etc/drwcsd.conf saved as /var/opt/drwcs/etc/drwcsd.conf.rpmsave
===> Removing (postun): Dr.Web(R) Enterprise Suite
===> Removing init.d script
===> Cleanup after all
===> Removing Dr.Web(R) Enterprise Suite: Done

Please enter the path to your ES backup data
  or just press Enter to use the default path (/var/tmp/drwcs)
  or enter 0 for the clean installation.

:
```

```
Please enter the path to your ES backup data
  or just press Enter to use the default path (/var/tmp/drwcs)
  or enter O for the clean installation.

:
Preparing...                  ######################################## [100%]
   1:drweb-esuite             ###########                             ( 26%)
```

```
Trying to restore old data from backup.
Backup directory "/var/tmp/drwcs" found.
Restore "/var/tmp/drwcs/dbinternal.dbs" --> "/var/opt/drwcs/dbinternal.dbs"
Restore "/var/tmp/drwcs/drwcsd.conf" --> "/var/opt/drwcs/etc/drwcsd.conf"
Restore "/var/tmp/drwcs/drwcsd.pri" --> "/var/opt/drwcs/etc/drwcsd.pri"
Restore "/var/tmp/drwcs/drwcsd.pub" --> "/opt/drwcs/Installer/drwcsd.pub"
Restore "/var/tmp/drwcs/enterprise.key" --> "/var/opt/drwcs/etc/enterprise.key"
Restore "/var/tmp/drwcs/agent.key" --> "/var/opt/drwcs/etc/agent.key"
Restore "/var/tmp/drwcs/certificate.pem" --> "/var/opt/drwcs/etc/certificate.pem"
Restore "/var/tmp/drwcs/private-key.pem" --> "/var/opt/drwcs/etc/private-key.pem"
8 file(s) restored from backup.
Converting drwcsd.conf ...
Backup "/var/opt/drwcs/etc/drwcsd.conf" --> "/var/tmp/drwcs/drwcsd.conf"
Upgrading existing database (if needed) ...
Making initial product revision ...
chkconfig setup...
=== Restoring additional configs.
Restore "/tmp/tmp.Nth18dgG7N/auth-ldap.xml" --> "/var/opt/drwcs/etc/auth-ldap.xml"
Restore "/tmp/tmp.Nth18dgG7N/auth-radius.xml" --> "/var/opt/drwcs/etc/auth-radius.xml"
Restore "/tmp/tmp.Nth18dgG7N/auth-ads.xml" --> "/var/opt/drwcs/etc/auth-ads.xml"
```

However, not all Unix family operating systems support the upgrade from version 10 to version 12.0 over the installed version.

In this case, follow the steps below.

1. Stop the anti-virus server.

2. If you want to use any of the files in the future (other than the files that will automatically be saved when the server software is uninstalled), then back up these files manually, for example, copies of report templates, etc.

3. Uninstall the server software (see "Uninstalling Dr.Web Server for UNIX®-like operating systems" in the Installation Manual) and agree to save file backups. To do this, just enter the path for saving them or accept the path offered by default.

4. Use the backup to install the Dr.Web Server version 12.0 according to the standard installation procedure. All saved configuration files and the embedded database (if the embedded database is used), will automatically be converted for use by server version 12.0.

5. If you saved any files manually, place them in the same directories in which they were located in the previous server version. For all the files saved from the previous server version, you must specify as the owner of the server files the user you selected when the new version of Dr.Web ESS server was installed (by default — drwcs).

6. Run the anti-virus server.

7. Configure the upgrade of the repository and upgrade it completely.

After the upgrade is complete, reconfigure the encryption and compression settings for the linked servers (see the Administrator Manual's "Configuring connections between Dr.Web Servers" section).

3. Transferring Dr.Web Agents from a Dr.Web Enterprise Security Suite 10 server

To transfer the previously installed Dr.Web Agents connected to the Dr.Web Enterprise Security Suite server 10.x/11.x to the installed and configured Dr.Web Enterprise Security Suite 12 server, you must configure the connection settings of the protected stations.

Dr.Web Enterprise Security Suite allows you to specify for the Dr.Web Agents the anti-virus servers to which they should connect. This feature is used both for ensuring the stability of the anti-virus network and for migrating Dr.Web Agents between servers.

The first step is to get the public encryption key of the server to which the agents will migrate. To get the key, go to **Administration → Encryption keys**, select the public key, and export it.
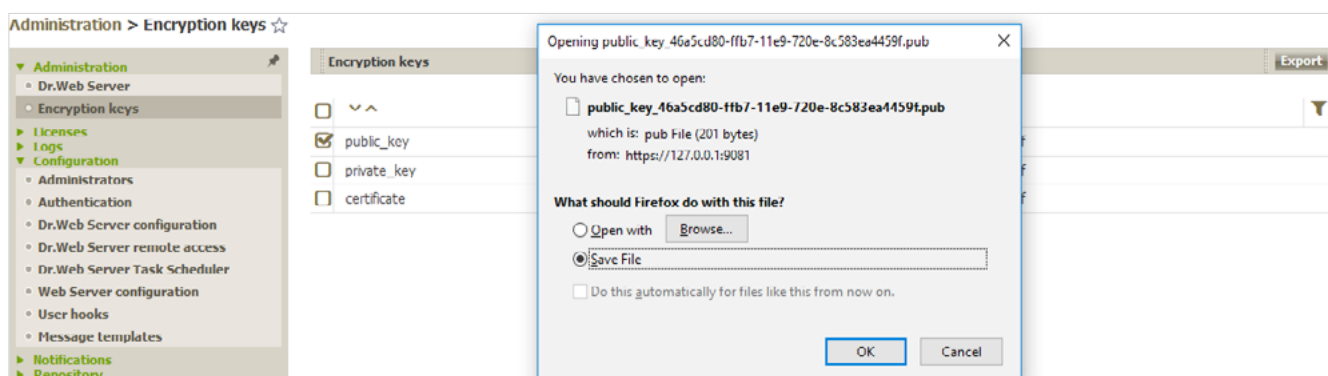
Next, go to the Dr.Web Enterprise Security Suite 10 server settings, and in the Network tab of the anti-virus server settings parameter, configure the parameters defining the settings for server interaction — the public key (in the field **Public key**) we exported earlier and the server address:
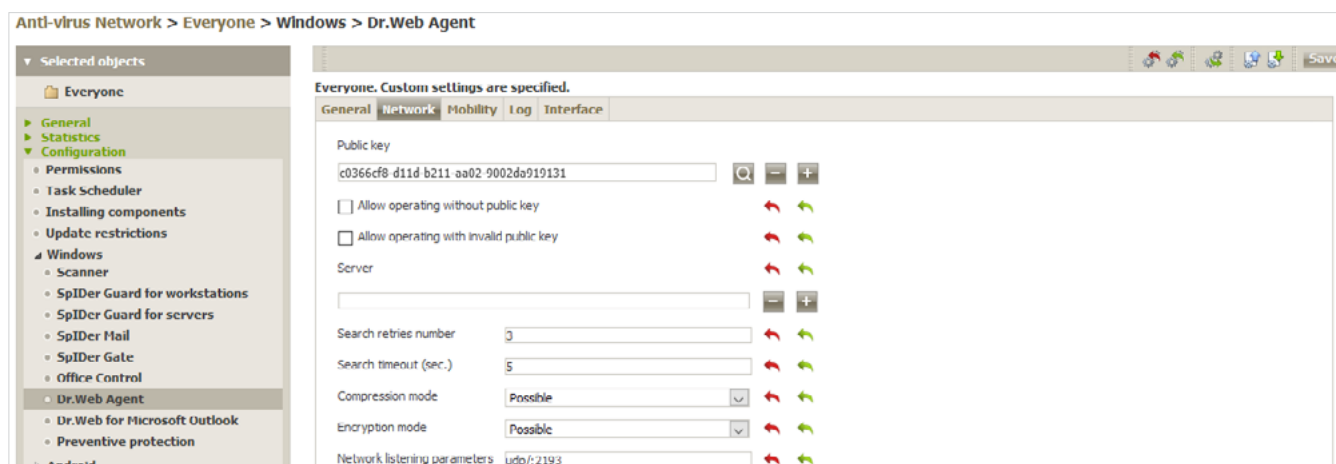
To replace the key file, click on the 🔍 button and select a key file. To add another public key, click on the ➕ button and select the key file.

In the **Server** field, specify the address of the anti-virus server to which the agents will migrate. You can specify one anti-virus server address or multiple addresses of different anti-virus servers.

To add another **Server** address click on the ➕ button and enter the address in the extra field. The format of the Server network addresses is described in the documentation.

Example on how to specify **Server** address:

    tcp/10.4.0.18:2193
    tcp/10.4.0.19
    10.4.0.20

Important! If you specified an invalid/incorrect **Server** parameter, the Agents will disconnect from the Dr.Web ESS server and will not be able to connect to it again. In this case, you should specify the server address directly on the station.

Important! In order to be able to change the connection settings on a workstation, when the transfer is being made, you need to give the station the right to **Change the configuration of Dr.Web Agent**. You can manage rules in the Control Center's **Rights** section.

After configuring the parameters, wait until the Dr.Web Agents appear in the list of the Anti-virus server network where the migration is being carried out and turn off the previously used server.

4. Upgrading Dr.Web Agents for stations running the Windows OS

The Agents supplied with Enterprise Security Suite version 10/11 are upgraded automatically.

If the Agents are installed on stations running operating systems that do not support the installation of Agents for Dr.Web Enterprise Security Suite version 12.0, no update actions will be carried out. The list of supported operating systems is available in the documentation.

The Agents are automatically upgraded if the encryption keys and network settings of the previous server were stored during the server upgrade process. The automatic upgrade requires manual configuration if new encryption keys and the previous server's network settings were specified during the server upgrade process.

The Agents installed on unsupported operating systems will not be able to receive upgrades (including virus database updates) from the new Dr.Web ESS server. If you need Agents on unsupported operating systems, you must leave as part of your anti-virus network the previous Server versions to which these agents are connected.

After the automatic update, you will then be prompted to reboot the system; in the Control Center, in the station status, the need to perform a restart after the upgrade is noted. To complete the upgrade, restart the station locally or remotely via the Control Center.

If the station is connected to the server via the Dr.Web Proxy Server Agent, before upgrading, you must upgrade the Proxy Server to version 12.0 or remove the Proxy Server.

4.1. Automatic upgrading of the Agents supplied with Dr.Web Enterprise Security Suite 6

The Agents are automatically upgraded if during the Dr.Web ESS server upgrade process the encryption keys and previous server's network settings were stored according to the following scheme:

1. When the upgrade process is launched, the old Agent version is removed.
2. The station is restarted manually.
3. The new Agent version is installed. For this, a task is automatically created in the Dr.Web ESS server schedule.
4. After the Agent is upgraded, the station is automatically connected to the server. In the Control Center's "Status" section, you will be prompted about the need to restart. You need to restart the station.

The automatic upgrade requires manual configuration if during the Dr.Web ESS server upgrade process new encryption keys and server network settings were specified according to the following scheme:

1. Manually change the connection settings to the new server and replace the public encryption key on the station.
2. After changing the settings on the station and connecting the station to the server, start the Agent upgrade process.

3. The old version of the Agent will be removed during the upgrade.

4. Restart the station manually.

5. The new version is installed. For this, a task is automatically created in the server schedule.

6. After the Agent upgrade is complete, the station is automatically connected to the server. In the Control Center's "Status" section, you will be prompted about the need to perform a restart. Restart the station.

During the automatic upgrade, note the following features:

- After the Agent is removed, a notification to restart the station is not displayed. The administrator must restart the station.

- During the interval between the old Agent version's removal and the new version's installation, the stations will be without anti-virus protection.

- After the Agent upgrade, the anti-virus software will operate in a limited fashion until the station is restarted. Until that happens, the station does not have full anti-virus protection. The user must restart the station when the Agent prompts them to do so.

If the installation of the new Agent version fails for some reason during the automatic upgrade, further installation attempts will not be made. The anti-virus software will not be installed on the station and in the Control Center, such a station will be displayed as disabled. In this case, you must install the Agent on your own. And, after installing the new Agent, you will need to combine the old and new stations in the Control Center, in the anti-virus network's hierarchical list.

5. Upgrading Dr.Web Agents for stations running the Android OS

Dr.Web Enterprise Security Suite 12.0 only supports Dr.Web Agent versions 12.2 and later for the Android OS.

On mobile devices, you must manually upgrade the Dr.Web Agents for Android to work with Dr.Web Enterprise Security Suite version 12.0.

Before upgrading the Dr.Web anti-virus server, manually upgrade the Dr.Web for Android Agents on mobile devices up to version 12.2 or higher.

Download the new version from Doctor Web's site at https://download.drweb.com/android.

The new Agent will connect to the previous anti-virus server version, and then you can upgrade the Dr.Web ESS server to version 12.0 in accordance with the general procedure.

If you cannot download the installation package of the Agent offline version via the Internet, after upgrading the Dr.Web Server, manually upgrade the Agents by downloading the installation package from the Control Center in the station properties or from the installation page. After upgrading the Dr.Web Agent server, Dr.Web for Android automatically connects to the upgraded server. After an upgrade attempt, the anti-virus protection will be disabled on mobile devices because the virus database versions will be incompatible. Upgrade the Agents manually, directly on mobile devices.

If you cannot download the installation package of the Agent offline version via the Internet and an error notification is undesirable on the mobile device, before upgrading the server, disconnect the Dr.Web for Android Agents from it. This way mobile devices will not be able to connect to the new Dr.Web ESS server to download incompatible updates. Upgrade the server to version 12.0 in accordance with the general procedure. Download the installation package from the Control Center in the station properties or from the installation page. Upgrade the Agent manually on mobile devices. Connect the upgraded Agents to the new server.

6. Upgrading Dr.Web Agents for stations running the Linux OS and macOS

The Agents installed on stations running Linux family OS and macOS connect to server version 12.0 if the following conditions are met:

1. The Agents must be installed on computers running operating systems under which Dr.Web Enterprise Security Suite version 12 Agents can be installed.
2. The encryption keys and network settings of the upgraded server should be specified on the stations.

If the software on stations is outdated, download the installation package of the new Agent version from the Control Center in the station properties or from the installation page. Upgrade the station software manually. If the latest version of the software is installed on stations, no other action is required.

7. Additional information

If you have any questions, including those related to the Dr.Web Enterprise Security Suite upgrade procedure, you can contact Doctor Web's technical support service for help.

Before contacting our technical support service for assistance, try to find the answer to your question by the following means:

- reading the latest versions of the descriptions and manuals at
  https://download.drweb.com/doc;
- reading FAQs at https://support.drweb.com/show_faq;
- visiting Doctor Web forums at https://forum.drweb.com.

If you are still unable to solve your problem, you can use one of the following methods to contact the Doctor Web technical support service:

- by filling out the request form at https://support.drweb.com/;

  To submit a request to the Doctor Web technical support service:

  - Follow the link: https://support.drweb.com/
  - Select the section that interests you and create a request (attach a serial number and a file with information if necessary).

Attach to your support request the report created by the dwsysinfo utility, which collects operational information on our solutions and on the operating system (no confidential information is collected). The link to the utility is:

http://download.geo.drweb.com/pub/drweb/tools/dwsysinfo.exe

To get a report, run the dwsysinfo utility on the server with administrator privileges, click on **Generate report**, and attach the archive created by the utility to your support request.

Wait for the support service's response.

- Call within Moscow: +7 (495) 789-45-86 or use the toll-free line for calls within Russia: 8-800-333-7932.
- Information on Doctor Web's regional offices can be found on the company's official website at https://company.drweb.com/contacts/offices/.