Dr.WEB®
since 1992

Dr.Web Enterprise Security Suite 12.0 Installing only Application Control and Dr.Web Scanner on a station

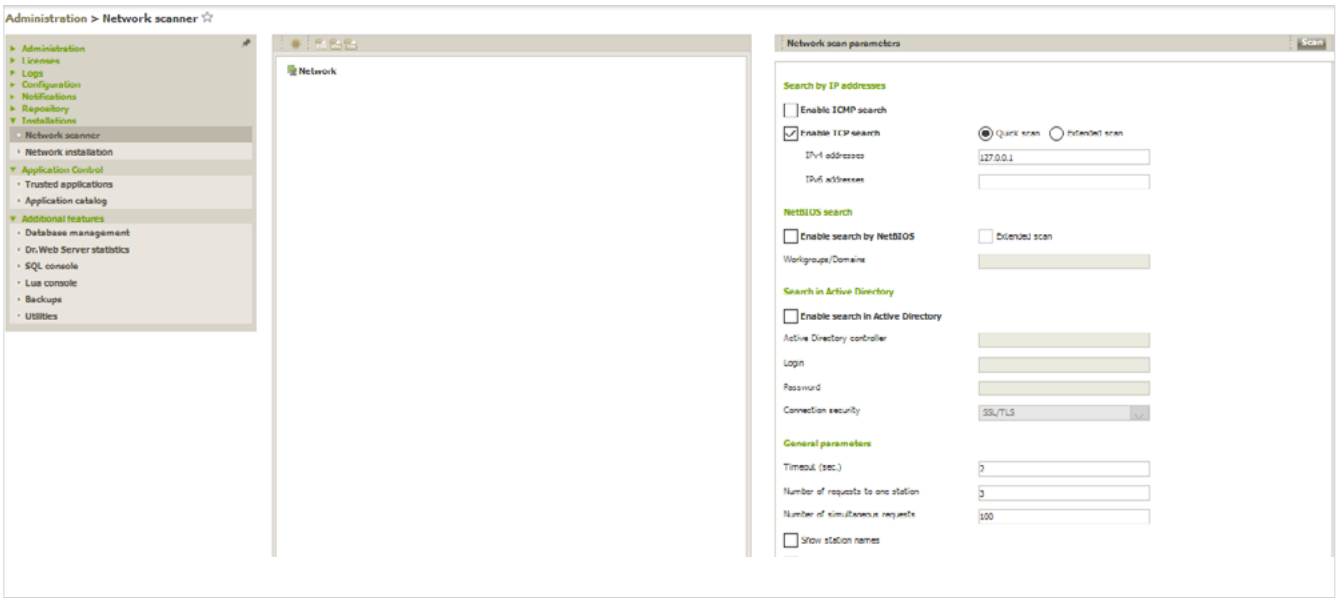
Dr.Web Enterprise Security Suite 12.0

Installing only Application Control and Dr.Web Scanner on a station

In some cases, it is not possible or desirable to use every component of the Suite—for example, in cases when a protected computer has a rather poor configuration or a computer's performance is critically dependent on its response time to certain events. Under these conditions, the **Application Control** and **Anti-virus scanner** modules can provide a computer with adequate protection. The former will be responsible for controlling the launch of only allowed applications (from the whitelist), and the latter will conduct regular anti-virus scans.

Let's take a closer look at the installation procedure for when only these two modules are installed. We use the **Network scanner** for installation.

Go to **Administration** → **Installation** → **Network scanner**.



The Network scanner does the following:

- Scans (browses) the network (including by IP addresses and NetBIOS) to detect workstations.
- Determines whether the Anti-virus **Agent** is installed on machines in order for request-response information to be exchanged via udp/2193 port (the default value). If packets sent to port 2193 are not accepted (e.g., they are blocked by the firewall), the Network scanner won't be able to detect the agent and will assume that the agent is not installed on the computer.
- The network scanner can use Active Directory and LDAP features to search for hosts. The machines can belong to different domains.

Important! It is not recommended to run the Network scanner under Windows 2000 and older versions— it may not be able to scan a network thoroughly.

The **Quick scan** parameter determines the network scan type. If **Quick scan** is enabled, the following actions are performed:

1. Ping requests are sent to machines on the network.
2. Requests to determine whether agents are available are sent to the hosts responding to ping requests.
3. Agents are detected using the standard routine.

Ping requests can be blocked due to network policies (for example, by the firewall). In this case, you can use an alternative method to determine which hosts have the agent up and running. If you use a standard search method, no ping requests are sent. Instead, hosts are probed for agent availability, one after another. This method can be used if ping requests are blocked because of network policies (if there are hosts on the network that have ping requests blocked (for example, if **Public network**, **Home network**, or **Cafe** is selected in Windows Vista and older versions, the firewall will block ping requests)). This method can be employed to supplement the quick scan. With Quick scan, requests are sent simultaneously, whereas with the expanded scan, requests are sent consecutively, which slows down scanning.

The maximum scanning time can be determined as follows:

- Standard scanning: *<N> * <timeout>* ,
- Quick scanning: *<N> / 40 + 2 * <timeout>* ,
  Here <N> indicates the number of hosts, and <timeout> is the value defined in the **Timeout** field.

In the **Network field**, enter the parameter of your network/networks as follows:

- separated by a hyphen (for example, 10.4.0.1-10.4.0.10);
- separated by a comma and a space (for example, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90);
- using a network prefix (for example, 10.4.0.0/24).

Change the port and timeout values, if necessary.

Click on **Scan**.

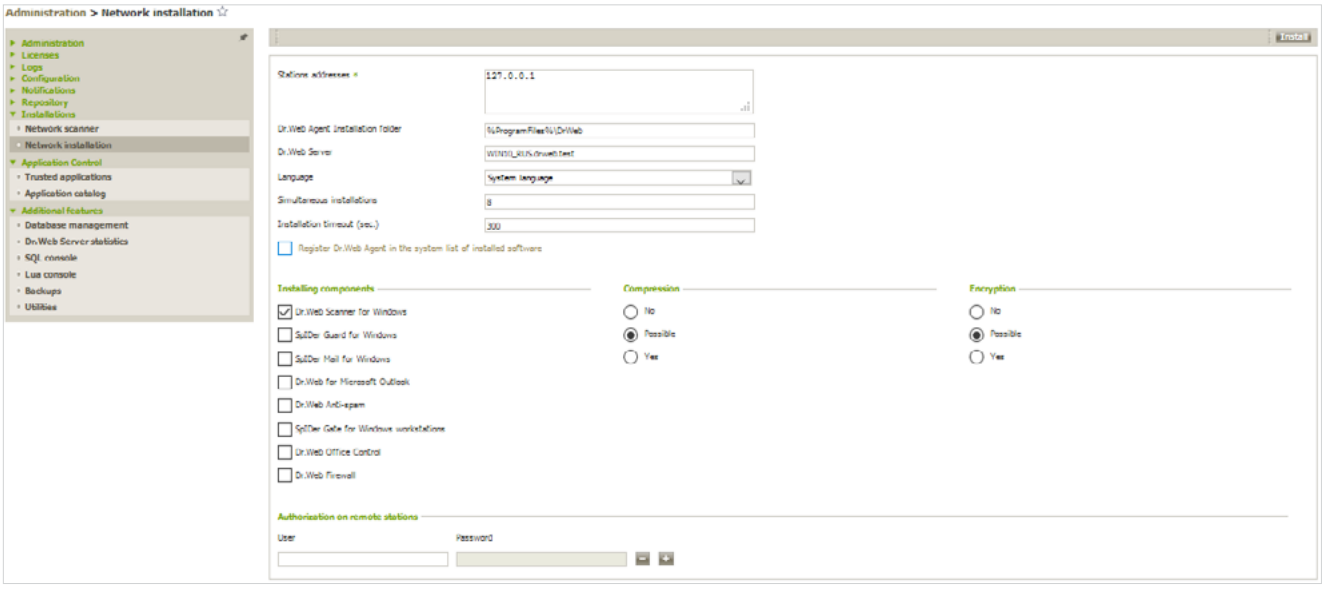
After scanning, the window will display a hierarchical list of computers and indicate whether the anti-virus software is installed on the machines. Icons are displayed next to all the listed items indicating workgroups and hosts. Information about the icons' meaning can be found in the documentation.

If necessary, you can expand the workgroup items on the list.

You can expand the entries that correspond to the hosts marked with the or icons to learn which anti-virus components are installed on the machines.

Clicking on the component icon for the host connected to this server will bring up the component settings window.

Select one or more unprotected stations and click on .



In the subsequent window, specify the installation parameters including the software components that you want to install.

In the **Stations addresses** field, you can specify the IP address of the computer(s) on which the anti-virus software will be installed. When you install the agent on multiple computers, you can specify multiple IP addresses as follows:

- separated by a hyphen (for example, 10.4.0.1-10.4.0.10);
- separated by a comma and a space (for example, 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90);
- with the network prefix (for example, 10.4.0.0/24).

You can also specify the hosts' domain names instead of IP addresses.

By default, in the **Server** field, the IP address or the DNS name of the **Dr.Web Server** to which the Dr.Web Control Center is connected is displayed. If necessary, specify the address of the server from which the anti-virus software will be installed.

In the **Authorization on remote PCs** section, you can specify the parameters for the agent's authorization on the Server. If the corresponding fields are left empty, the authorization parameters will be set automatically.

In the **Encryption** and **Compression** sections, you can enable the encryption and compression of traffic between the Agent and the Server.

In the future, these parameters can be changed in the **Agent** settings and in the host properties.

To install, select only Dr.Web Scanner for Windows.

Click on **Install**.

Important! To remotely install the agent on a host, the directory admin$\TEMP must be accessible from the server. If access is unavailable, the installation will fail. Access to the directory can be blocked by UAC.

Important! Once the managing network account settings are changed, you need to restart the host for the changes to take effect.

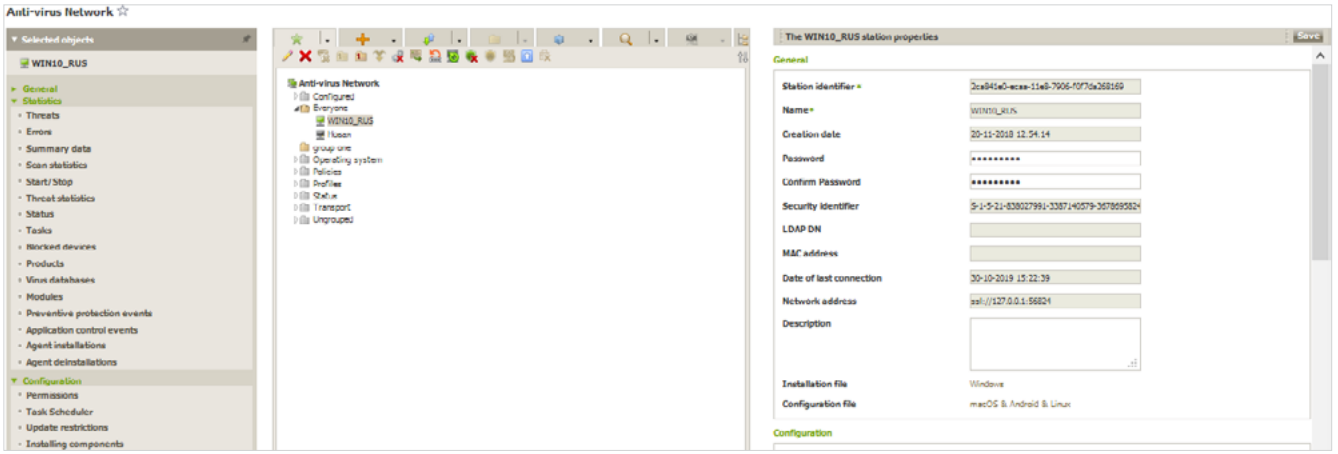
With the default Dr.Web Server settings, the administrator must manually approve new hosts in order for them to be registered on the Server (for more on new host policies, refer to the New Host Policies section). In this case, new hosts are not connected to the Server automatically but are added to the **New** category of the **Status** group.

The installation procedure takes some time since the product's integrity is verified during installation, new components are downloaded from the Server, and components are copied into the repository and installed from the repository with a post update. While all the necessary files are being downloaded, update error report notifications will be displayed and the host will be placed in the subgroup **Update Errors** of the Stations group. Once installation is complete, the status will change automatically. It is not recommended to update all the components/failed components. That would only result in the message **Operation initiated** being displayed.

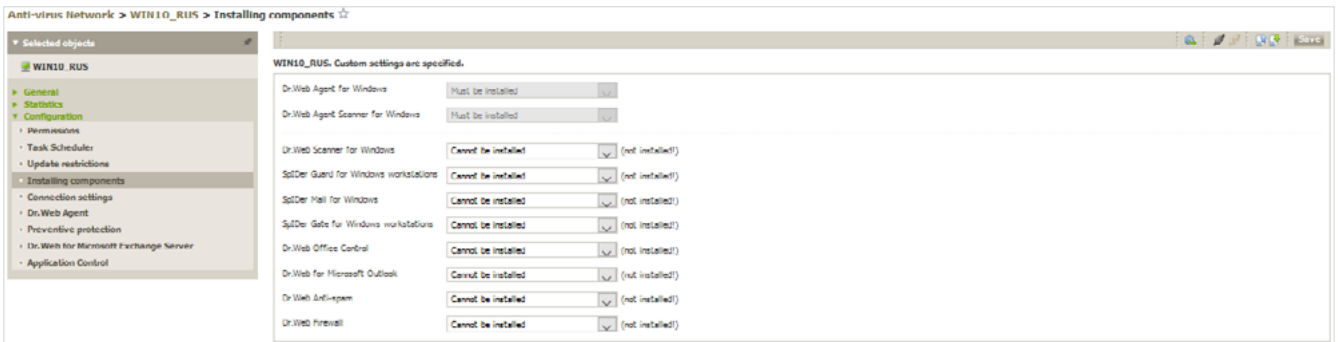
To finish installing some of the anti-virus components, you may need to restart the computer. In this case, you will see an exclamation mark in a yellow triangle against the **Agent** icon in the system tray or (for earlier versions of Windows) the setup will bring up the corresponding prompt.

If necessary, you can also remove anti-virus components, leaving only the Application Control and Anti-virus Scanner modules.

To do this, choose the desired groups or individual stations, and go to the **Installing components** section.

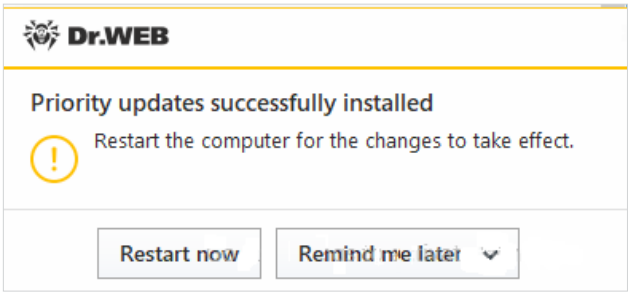


In the drop-down lists, select **Cannot be installed** for all the components available for removal.

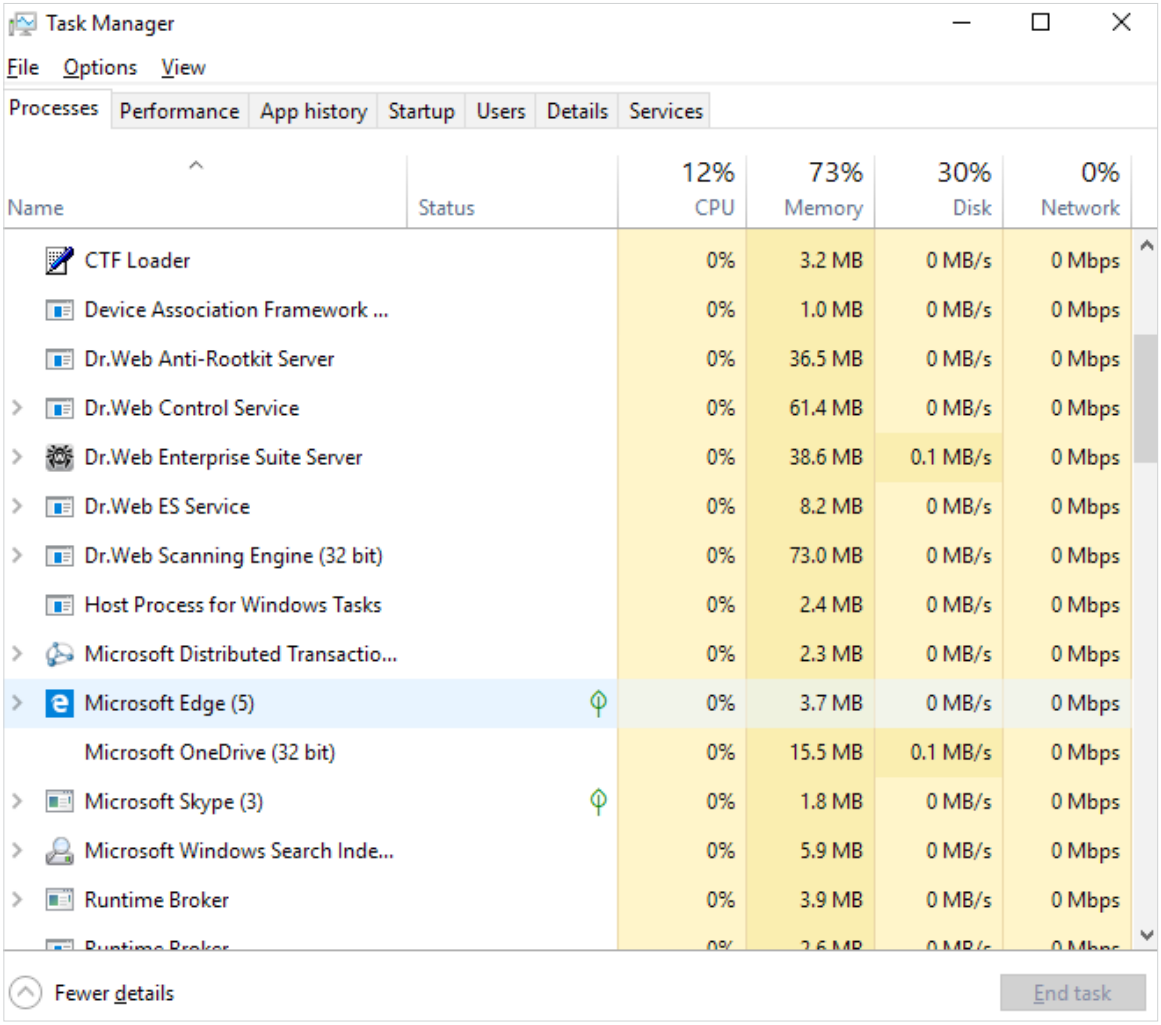


Click on **Save**.

The modules will be removed, and you will be prompted to restart the system, if necessary.



If you open the **Task Manager** after the restart, the list of processes will only contain the processes of the scanning module and the anti-virus agent. Note that the presence of these two processes does not affect PC performance because the resident anti-virus protection is absent.



Doctor Web
2003–2019

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Tel.: +7 (495) 789–45–87
Fax: +7 (495) 789–45–97

https://www.drweb.com | hhttps://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com