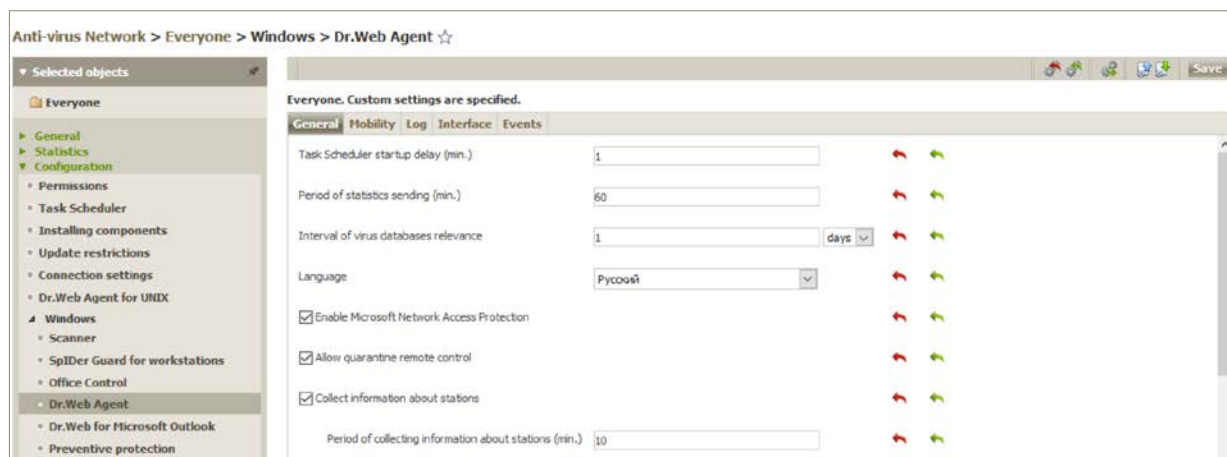# Dr.WEB®
since 1992

NEW VERSION 11

Control system software and hardware information with Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite can aggregate and store information about the software and hardware being used on protected Windows hosts.

To reduce traffic, the Dr.Web option to gather hardware and software information is disabled by default.

In the control menu, select **Configuration → Windows → Dr.Web Agent**. In the General tab, tick the box next to **Collect information about stations**. Use the **Period of collecting information about stations** option to specify how often the agents are to send system information to the server.

To enable the feature, in the main menu select **Administration → Dr.Web Server Configuration**. Go to the **Statistics** tab, and tick the box next to **Hardware and software** so that the information will be written into the log and server database.

In the control menu's **General** tab, select **Hardware and software**.

Adjust the table view parameters:

- Click the gear ⚙ icon, and specify the columns that are to be displayed.
- Click on the ▼ icon to run a search in all the table's columns.

You can also export host software and hardware information into a file.

An anti-virus network administrator can look for network hosts using the hosts' hardware and software as search criteria.

To monitor the security status for specific hosts, select the hosts in the network view, and in the menu on the left, select **Statistics → Status**.