Dr.WEB

AV-Desk

Release Notes

Dr.Web AV-Desk
Version 13.0
Release Notes

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web anti-virus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Release Notes for Dr.Web AV-Desk 13.0 5
New in Current Release of Dr.Web AV-Desk 13.0 5
New in Dr.Web AV-Desk 13.0 6
Upgrading the Dr.Web AV-Desk Components to Version 13.0 11
Technical Support 13

Release Notes for Dr.Web AV-Desk 13.0

The present document contains a history of the most critical changes in Dr.Web AV-Desk 13.0. Detailed information about the anti-virus network based on Dr.Web AV-Desk, including installation and component configuration details, is available in manuals from the administrator documentation package.

New in Current Release of Dr.Web AV-Desk 13.0

New Features and Improvements

- You can now create a virtual agent to protect virtual environments.
- Now you can adjust settings of automatic statistics cleanup for Dr.Web Agent for Windows and quarantined objects deletion after a specified time period, using the corresponding options in **Anti-virus Network** → **Dr.Web Agent** → **General** in the Control Center. Adjusted settings can be applied on any stations with Dr.Web Agent for Windows installed that supports this feature.
- From a user group properties in the Control Center's anti-virus network tree, you can now separately download a configuration file that includes Dr.Web Server connection parameters for any stations in the group running macOS, Android or Linux.

Important Changes

- Any group or personal installation packages of Dr.Web Agent for macOS available in the Dr.Web Server's repository or generated from the Control Center now have the `.run` extension. The `.cdr` packages are no longer supported by Dr.Web Server. Once you update Dr.Web Server, make sure to update the Dr.Web for macOS product from **Administration** → **General repository configuration** in the Control Center.

Resolved Issues

- Fixed an error that sometimes would not let an administrator change the password for accessing the Control Center.
- Fixed an error that made it impossible to remove associated Dr.Web Proxy Server from a station properties window in the Control Center.
- Fixed errors related to Dr.Web Server restart notification appearing after changes are made in **Administration** → **Authentication** in the Control Center.
- Fixed errors that occurred when working in the Control Center from Internet Explorer 11.
- Fixed errors that occurred in **Administration** → **User hooks** in the Control Center.
- Fixed a number of errors that occurred when handling the license keys in the Control Center.
- Fixed a number of errors that occurred in **Anti-virus Network** → **Quarantine** in the Control Center.

- Resolved an issue, due to which group administrators were granted excessive access rights.
- Resolved an issue that caused an error when a group administrator tried to view statistics in reports.
- Optimized resource consumption when running SQL queries when creating the anti-virus network tree.
- Improved handling of API operations with groups.
- Optimized operation with large amount of groups and stations in tree.
- Other minor corrections.

New in Dr.Web AV-Desk 13.0

New Features and Improvements

New Components

- *Application Control* is a new available component that allows you to adjust which applications to permit and which ones to prohibit from launching on protected workstations in the anti-virus network, on which Dr.Web Agent for Windows is installed. The component can be configured on Dr.Web Server only.

Dr.Web Server

- Several new products are now available in the repository: **Dr.Web enterprise products** and **Dr.Web administrative utilities** containing installation packages of different products, components and utilities, as well as **Documentation** containing a full set of manuals describing the Dr.Web anti-virus network. Installation packages for Dr.Web enterprise products are available in the similarly named section of the Control Center (**Administration** → **Enterprise products**). A full list of packages becomes available after setting up the repository.
- Dr.Web Agent for UNIX can now be installed remotely. The installation can be performed from the **Administration** → **Network installation** section of the Control Center or using a standalone utility.
- New redesigned principle of network scanning and remote installation of the Agents (web browser extension is no longer used).
- Web API that is used for interaction with Dr.Web Server has been updated to version 4.3.0. Administrator groups can now be created via Web API.
- A new feature allowing administrators to receive notifications about any events from workstations connected to neighbor Dr.Web Servers.
- Dr.Web Proxy Server can now update automatically if connected to Dr.Web Server.
- The process of Dr.Web Server repository update from GUS has been remade. The process can now launch and provide information about progress and update status in real time.

- The number of settings for remote management of workstations running UNIX system-based OS has been extended. Settings from the unified configuration file of anti-virus components can now be adjusted remotely.
- A new Server extension is now available that is called Dr.Web SNMP agent. It is intended for exchanging information with network management systems via the SNMP protocol.
- Default administrator (*admin*) password can now be specified in the configuration file with answers to install the Server on a UNIX system-based OS.
- Windows Server 2019 is now supported by both Dr.Web Server and Dr.Web Agent for Windows.
- MySQL version 8 is now supported and can be used as an external database.
- Administrator password is now encrypted with a cryptographic salt by default. You can view or change a randomly generated salt value in the Server configuration file.

Dr.Web Security Control Center

- The **Reports** section has been redesigned.
- A number of new utilities are now available in the **Administration** → **Utilities** section:
  - *Dr.Web Agent for Windows remote installation utility* and *Dr.Web Agent for UNIX remote installation utility* intended for remote installation of the Agent on workstations running the corresponding operating systems.
  - *Dr.Web for Windows removal utility*, which is an emergency tool for removing incorrect/damaged installations of Dr.Web Agent for Windows software when standard removal tools are unavailable or will not work. The utility is not designed to be used as the main Dr.Web software uninstallation tool.
  - *Dr.Web utility for collecting information on a system* that is intended for generation of the report about the state of system and all installed software, including Dr.Web anti-virus solutions for protected stations and Dr.Web Server software. The report archive can be used for diagnostics by anti-virus network administrator or can be submitted to the Doctor Web technical support service.
- License agreement has been updated.
- **License usage report** is now available in the **Administration** section of the Control Center's control menu. This report contains information about all licenses used by the current Server and any neighbor Servers.
- **Detected hardware** is now available in the **Anti-virus Network** section of the Control Center's control menu. This new section contains details about the hardware detected on workstations. This data is collected after the corresponding setting is enabled in configuration of both the Server and Agent.
- A new log type is added, with information about abnormally terminated connections of Dr.Web Server with the clients.
- The anti-virus network groups are now able to automatically synchronize with Active Directory on UNIX system-based OS. Active Directory connection settings were added to make the corresponding task available in Dr.Web Server Scheduler.

- A new feature to inform administrator when any security threats from the list of known hashes of threats are detected. Information about such threats is displayed in scanning statistics and corresponding administrator notifications. Also, a manual search among the list of known hashes is now available. Bulletins of known hashes of threats are stored as a new repository product and licensed separately.
- Dr.Web Firewall parameters for workstations running Windows OS can now be configured in the Control Center.
- The detailed repository configuration has been extended with the settings **Prevent sending updates to neighbor Servers** and **Prevent receiving updates from neighbor Servers** that allow to disable sending or receiving the product updates via the interserver connections.
- Multiple improvements were made to the **Parental Control** component. The Parental Control settings can now be configured for specific user groups; new web filter categories were added; new flexible access right controls for third-party devices are now available.
- **Message templates** are now available in the **Administration** section of the Control Center's control menu. This new section lets you create and save templates of messages to send to the anti-virus network workstations. When necessary, the same section can be used to send a message to the workstations.
- Several new log types are now available in the **Administration** → **Logs** segment of the control menu:
  - *Real-time log* keeps any events and changes in the Server operation as they happen.
  - *Message log* saves all the messages administrator sends to protected workstations.
  - *Log of abnormally terminated connections* contains information about any cases of disconnection between the Server and the clients: workstations, neighbor Servers, and Proxy Servers.
- A new feature to specify the number and percentage of CPU cores to be used when scanning workstations running Windows OS.
- A list of administrator user hooks' parameters has been extended.
- A new option in the **Update restrictions** section is now available that allows to disable Agent downgrade when downloading available revisions from the Server.
- In the Control Center, the list of supported settings for Dr.Web ICAPD and SpIDer Gate for workstations running UNIX OS has been extended.
- A new feature allowing to remotely start and stop protection components for workstations running UNIX system-based OS.
- New options were added to Dr.Web Server and Web Server configuration that allow preliminarily create and configure Lua virtual machines for operating with a corresponding component.
- A new option in Dr.Web Server configuration that allows to automatically create missing workstation accounts when installing the Agents using a group installation package.
- New settings for grouping Dr.Web Server notifications for Preventive protection, Application Control, epidemics and abnormally terminated connections with clients.
- The INI configuration file for protection components for workstations running UNIX system-

based OS can now be exported and imported.

- The XML file containing workstation group membership rules can now be exported and imported.
- In the anti-virus network tree, workstations can now be searched by MAC address.
- A new setting is now available in the Dr.Web Agent for Windows configuration that allows to transmit information about geographical location of workstations to the Server.
- Dr.Web Agent for UNIX settings now include an option allowing to collect information about hardware and software installed on a workstation.
- A new setting is now available in the Dr.Web Agent for Windows configuration that allows screen readers to be used in the Agent interface on protected workstations.
- You can now set automatic restart parameters for a workstation after remote uninstallation of Dr.Web Agent for Windows using the Control Center.
- In the Control Center, you can now create a group installation package of Dr.Web Agent for Android if necessary.
- Lost administrator password can now be recovered from the Control Center.
- The anti-virus network tree has been completely remade. The new tree is able to display even more objects, at no cost in sorting speed or ease of navigation.
- A new section of the server statistics is now available with the Web Server access parameters.
- A new statistics type is now available about the events detected on workstations by the Preventive protection component.
- A new statistics type is now available about the disk space on protected workstations, including information about present logical drives and free space. The statistics is collected once the corresponding setting is enabled in the Server configuration.
- A new statistics type is now available about the devices blocked by protection components on the anti-virus network workstations.
- The **Modules** statistics section now includes information about the workstations running a UNIX system-based OS.
- In the repository settings, the update folder path on GUS servers (aka *Base URI*) has been changed to `/update`.
- In the settings of the SpIDer Guard for workstations component, the following threats are now set to be reported by default, when detected: *Jokes*, *Riskware*, and *Hacktools*.
- The **Help** section now allows to open the Administrator manual directly or proceed to the **Support** section where you can find links to support resources and documentation in HTML and PDF. The PDF documentation becomes available after setting up the repository.
- The Cloud Checker component for workstations running Android OS has been renamed to **URL filter** and now it includes a new category allowing to block access to cryptocurrency mining pools.
- The SpIDer Gate web filter categories have been extended with *Anonymizers*, *Online games*, *Cryptocurrency mining pools*, and *Jobs*.
- A new approach for using policies when configuring the workstations. The changes have

affected the rules of creating policy versions and assigning licenses to policies and policy groups via License Manager.

- In the **Administration** → **Backups** section, now you can see not only backups from the `var/backups` directory, but all the backups created in Dr.Web Server Task Scheduler.

Dr.Web Agent

- Dr.Web Agent software for Android OS can now update automatically when connected to the Server and notified of a new version available.
- A new Agent extension is now available for file data transferring from the Agent to the Server via the SFTP protocol.
- Dr.Web Agent for Windows is now capable of throttling the rate of data transfer with the Server.
- Dr.Web Agent graphical interface has been completely redesigned.

Resolved Issues

- Fixed an error, due to which in some cases Dr.Web Server was unable to be properly configured for operation through a proxy server (the **Administration** → **Dr.Web Server configuration** → **Network** → **Proxy** section of the Control Center).
- Fixed an error that caused Dr.Web Server crash when set up with the PostgreSQL external database and received data in invalid encoding from protected workstations.
- Fixed an error in archive creation when exporting the repository using the Dr.Web Repository Loader utility.
- Fixed a filtering error when displaying objects in the **Quarantine** section of the Control Center.
- Fixed Dr.Web Server update error that occurred on FreeBSD/i386 when trying to update via GUS.
- Fixed an error that prevented Dr.Web Agent from being installed using an installation package on devices equipped with the CPUs with no SSE2 instruction set support.
- Fixed a number of errors in the administrator notifications.
- Resolved an issue, due to which Dr.Web Server service could not start on some versions of Windows OS after restarting the computer.
- Resolved an issue that made Dr.Web Server inoperable on operating systems with invalid name of the system locale.
- Other numerous corrections.

Stopped Supporting

- Operating systems earlier than Windows 7 for x32 and Windows Server 2008R2 for x64 are no longer compatible with Dr.Web Server.
- The Dr.Web Server *extra* distribution kit is no longer provided. All the components coming

with it before are now available in the new **Enterprise products** section.

- Dr.Web Server can no longer be installed on logical drives with file systems that do not support symbolic links, in particular, the FAT family.
- The list of installed components of Dr.Web Server can no longer be changed via the installer.
- Connection to external databases that are not supported by Dr.Web Server is no longer possible.
- Propagation of a blocked license key to anti-virus network objects from the License Manager is no longer possible.
- The **Receive SMS commands without a password** option was removed from configuration settings of the workstations running Android OS.
- The **Enable hardware virtualization** option was removed from configuration settings of the workstations running Windows OS.

Known Issues

- Upgrading the Server on a UNIX-system based OS from version 10.1 to 13 via the Control Center is impossible when the owner of the `/opt/drwcs` folder is specified as `root` and not `drwcs`. In this case, before initiating the upgrade, make sure to manually change the `/opt/drwcs` folder's owner to the `drwcs` user and the `drwcs` group. See example of the required command in the notes of the **Upgrading Dr.Web Server for UNIX System-Based OS** section of the **Installation Manual**.
- The `drwrawsocket` file that is required for Network Scanner will be missing after upgrading the Server on a UNIX-system based OS from version 10.1 to 13 via the Control Center. For a solution, see notes in the **Upgrading Dr.Web Server for UNIX System-Based OS** section of the **Installation Manual**.
- Some unsupported repository products can be transferred through interserver connection between the Servers of version 10 and 13 during the upgrade. Specifically, old products that are no longer included in the new Server repository, or any new products that are not included in the old Server repository. As a result, you can get an update error due to unknown product present in the repository. In the **Repository content** section, such products have their location directory stated as their name instead of normal product name.
- After setting up the repository and downloading the PDF documentation from the GUS servers, the documentation will be displayed in the **Help** → **Support** section of the Control Center only once the Server is restarted.
- Any manually created user hooks will not be saved as the result of the Server upgrade.

Upgrading the Dr.Web AV-Desk Components to Version 13.0

The upgrading procedure for Dr.Web anti-virus network components has a number of critical points. Before any upgrading activities, make sure to read through the **Upgrading Dr.Web AV-Desk Software and Its Components** section of the **Installation Manual**.

Upgrading Dr.Web Server for Windows OS

- The Server upgrade from version 10 to and within version 13 is performed automatically via the installer.
- The Server can also be upgraded from version 10 to version 13.0 via the Control Center. This procedure is described in the **Administrator Manual**, in the **Updating Dr.Web Server and Restoring from the Backup** section.

Upgrading Dr.Web Server for UNIX system-based OS

- The Server upgrade from version 10 to and within version 13 for the same package types is performed automatically on all UNIX system-based OS via the installer. You can also upgrade the Server manually, if needed.
- The Server can also be upgraded from version 10 to version 13.0 via the Control Center. This procedure is described in the **Administrator Manual**, in the **Updating Dr.Web Server and Restoring from the Backup** section.

Upgrading Dr.Web Agent for Windows OS

The Agent supplied with AV-Desk 10 is upgraded automatically. After the automatic upgrade, a pop-up notification with restart request is displayed on a station; in the Control Center, the restart request is displayed in the station status. Restart the station locally or remotely via the Control Center to complete the upgrade.

Upgrading Dr.Web Agent for Android OS

- Starting from version 12.6.4 Dr.Web Agent for Android is upgraded automatically, once notified of a new version available.
- If necessary, the Agent can also be upgraded manually by uploading a new version of installation package to a device via the Control Center after the Server is upgraded to version 13. The installation packages become available once you set up the repository. See details in the **Installation Manual**, in the **Installation Files** section.

Upgrading Dr.Web Agent for Linux OS and macOS

- The Agent for Linux OS can be upgraded via the official Dr.Web repository. This procedure is described in **Dr.Web for Linux User Manual**, in the **Installing and Uninstalling** → **Upgrading Dr.Web for Linux** section.
- The Agent for macOS can be upgraded manually by uploading a new version of corresponding installation package to a workstation via the Control Center once the Server is upgraded to version 13. The same method can be applied for the Agent for Linux OS. The installation packages become available once you set up the repository. See details in the **Installation Manual**, in the **Installation Files** section.

Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at https://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at https://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.