Dr.WEB

for macOS

User Manual

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web for macOS
Version 12.0
User Manual
1/22/2021

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

1. Dr.Web for macOS 6

1.1. Document Conventions 6

1.2. About Dr.Web 6

1.3. System Requirements 7

2. Installation and Uninstallation 8

3. Managing Licenses 11

3.1. Trial Version 11

3.2. Purchasing License 11

3.3. License Activation 12

3.4. License Renewal 14

3.5. License Restoration 15

3.6. Serial Number 15

3.7. Key File 16

4. Dashboard 18

5. Notifications 20

6. Updating Virus Databases 21

7. Real-Time File System Protection 23

7.1. Configuring SpIDer Guard File Monitor 24

7.2. Excluding Files and Directories From Scanning 26

8. Web Traffic Scan 27

8.1. Configuring SpIDer Gate Internet Monitor 28

8.2. Excluding Websites From Scanning 31

8.3. Encrypted Traffic Scan 31

8.4. Excluding Applications From Scanning 32

9. Protection From Network Threats 34

9.1. Firewall Preferences 35

10. Scanning Mac on Demand 38

10.1. Scanner Preferences 40

10.2. Excluding Files and Directories From Scanning 43

11. Privacy Protection 45

11.1. Allow Access to Camera and Microphone 45

12. Neutralizing Threats 47

12.1. Threats 47

12.2. Quarantine 48

13. Support 50

13.1. Help 50

13.2. Questions and Answers 50

13.3. Error Codes 54

13.4. Technical Support 59

14. General Preferences 60

15. Connection to Cloud Services 62

16. Central Protection Mode 63

17. Reference Information 67

17.1. Central Protection and Anti-Virus Network 67

17.2. Threat Types 69

17.3. Detection Methods 73

17.4. Keyboard Shortcuts 76

1. Dr.Web for macOS

1.1. Document Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
⚠	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`/Volumes/Macintosh HD/`	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

1.2. About Dr.Web

Dr.Web for macOS protects Mac from various types of threats: viruses, rootkits, trojans, spyware, and adware using the most advanced virus detection and neutralization technologies.

Dr.Web components are constantly updated. New threat signatures are regularly added to the virus and website category databases. Updates provide an up-to-date level of device protection. To neutralize unknown threats, heuristic analysis methods are implemented.

Main functions

- real-time scan of all files on your Mac,
- system scan on demand,
- scan of data transmitted via an insecure HTTP protocol,
- monitoring network connections of applications and blocking suspicious connections,
- protection of cameras and microphones from unauthorized access.

Program information

To open the program information window, click in the main window.

The information is specified in the following tabs:

- **About Dr.Web**—program version, last update date, scan engine version.
- **Help**—help describing program operation.
- **News**—latest news published on the Doctor Web website.
- **Promotions**—Doctor Web promotional actions.
- **About Viruses**—news about viruses detected by Doctor Web virus analysts.

1.3. System Requirements

To install Dr.Web, you need:

- Mac running macOS operating system.
- About 2 GB of disk space.

List of supported versions

- OS X 10.10 Yosemite,
- OS X 10.11 El Capitan,
- macOS 10.12 Sierra,
- macOS 10.13 High Sierra,
- macOS 10.14 Mojave,
- macOS 10.15 Catalina.

How to check the version of Mac operating system

1. Choose the Apple menu .
2. Click **About This Mac**.
3. On the **Overview** tab, you'll see the version number right under the operating system name.

How to check the disk space on your Mac

1. Choose the Apple menu .
2. Click **About This Mac**.
3. Then choose the **Storage** tab. You'll see an overview of your free space.
4. Click the **Manage** button to see the recommendations for optimizing your storage.

2. Installation and Uninstallation

Dr.Web Installation

1. Download the installation file at https://download.drweb.com/mac/.
2. Run the installation file.
3. Click **Install Dr.Web**.
4. Click **Next**. The installation process starts.
5. Enter your user name and the password and click **Install Helper**.
6. Dr.Web for macOS will be copied into the **Applications** folder and start automatically.

After the installation is completed, the Dr.Web icon in the top macOS ribbon appears. It opens the Dr.Web main window.

During the first launch, Dr.Web updates virus databases to the current state. Dr.Web then updates virus databases every 30 minutes. You can change the update frequency.

Installation errors

Unsupported Operating System

Dr.Web for macOS is compatible with computers running supported version of macOS operating system. Please update your operating system.

How to check the version of Mac operating system

1. Choose the Apple menu .
2. Click **About This Mac**.
3. On the **Overview** tab, you'll see the version number right under the operating system name.

Not Enough Disk Space

To install Dr.Web, you need to have about 2 GB of disk space.

How to check the disk space on your Mac

1. Choose the Apple menu .

2. Click **About This Mac**.
3. Then choose the **Storage** tab. You'll see an overview of your free space.
4. Click the **Manage** button to see the recommendations for optimizing your storage.

Another Anti-Virus Installed

Dr.Web is not compatible with other anti-virus software including its own earlier versions. You also cannot install two versions of Dr.Web on one Mac.

Installing two anti-virus programs on one computer may lead to system crash and loss of important data. That's why you should uninstall the previous Dr.Web version on other anti-virus installed on your Mac.

See how to uninstall third-party anti-virus programs in the reference materials or on the official websites of the corresponding applications.

Error

Contact Doctor Web technical support. Attach the installation log stored in `\Library\DrWeb` to your request.

Error list

Dr.Web Uninstallation

1. Find the **Dr.Web Uninstallation** program using **Finder** and run it.
2. Enter your user name and the password.
3. Dr.Web for macOS will be uninstalled from the **Applications** folder.

> ⚠ During Dr.Web uninstallation the key and configuration files, as well as the file with program preferences are not removed from your Mac.
>
> Do not use third-party applications to uninstall Dr.Web. It may lead to incomplete uninstallation of the program.

If the program is not completely uninstalled, you can uninstall it manually.

To uninstall Dr.Web manually

Run the following commands in **Terminal** one by one:

- `sudo /bin/launchctl remove com.drweb.pro.configd`
- `sudo rm -f /Library/PrivilegedHelperTools/com.drweb.agent`
- `sudo rm -f /Library/LaunchDaemons/com.drweb.agent.plist`
- `sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove /Library/Application Support/DrWeb/bin/drweb-gated`
- `sudo /usr/libexec/ApplicationFirewall/socketfilterfw --remove /Library/Application Support/DrWeb/bin/drweb-firewall/bin/sleep`
- `sudo /sbin/kextunload -m com.drweb.kext.DrWebNetMonitor`
- `sudo /sbin/kextunload -m com.drweb.kext.DrWebMonitor`
- `sudo /bin/launchctl remove com.drweb.agent`
- `sudo rm -Rf "/Library/Application Support/DrWeb/lib"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/bin"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/cache"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/update"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/var"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/www"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/version"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/bases"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/dws"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/html"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/mail"`
- `sudo rm -Rf "/Library/Application Support/DrWeb/install.plist"`
- `sudo rm -Rf /var/log/drweb-agent.log`

3. Managing Licenses

License is necessary for Dr.Web operation. You can purchase it on the Doctor Web website or through authorized partners. The license allows you to use all program features during the whole license period. User rights are set in accordance with the License Agreement, which conditions users accept during the program installation.

Each license has a unique serial number, and a special file with license parameters is stored locally on the computer. This file is called a key file.

If you want to learn more about Dr.Web for macOS features before purchasing it, you can activate a trial version. All program functions and protection components are available in the trial version.

3.1. Trial Version

If you want to learn more about Dr.Web for macOS features before purchasing it, you can activate a trial version. It provides you with full functionality of the main components, but the trial period is restricted.

> ⚠ You can activate a trial version on the same computer no more than once a year.

You can activate a trial version:

- For 1 month. You don’t need to register or to have a serial number. License is automatically activated.

To activate a trial version

1. In the Dr.Web menu, select **License**.
2. In the **License Activation** section, select **Get a 30 day trial**.

3.2. Purchasing License

If you don’t have a valid Dr.Web license, you can purchase a new one in the Doctor Web online store.

To buy a new license

1. In the Dr.Web menu, select **License**.
2. Click **Buy**. Complete your purchase on the Doctor Web website.

When the purchase is completed, you'll get an email with a serial number or an attached key file.

3.3. License Activation

To get access to all program functions and components, activate your license. We recommend you to activate your license right after program installation. It's necessary for virus databases update and operation of program components, for example, real-time file system protection, protection from network threats, and web traffic scan.

When you run Dr.Web for the first time, activation starts automatically. You can also activate your license in the **License** section of the main program window. You can activate your license using a key file or a serial number.

How to activate your license using a serial number

1. In the Dr.Web menu, select **License**.
2. Click **Activate**.
3. In the **License Activation** window, enter your serial number.
4. Click **Activate**.
5. In the registration form, enter your name, region, and email. If necessary, you will be able to recover your license using this information. Click **Register**.
6. If you previously used a licensed version of a Dr.Web product for 3 months or more, you can specify its serial number, and the license period of your new license will be extended by 150 days as a bonus.
   - Click **Specify** if you already have a serial number of your previous license. Enter its number and click **Next**.
   - Click **Skip** if you don't have a serial number of the previous license.

How to activate your license using a key file

1. In the Dr.Web menu, select **License**.
2. Click **Activate**.
3. In the **License Activation** window, open the **Activation Files** tab.
4. Drag the key file in the `.key` format to the dotted area or click to choose the file on your Mac.
5. In the registration form, enter your name, region, and email. If necessary, you will be able to recover your license using this information. Click **Register**.
6. If you previously used a licensed version of Dr.Web for 3 months or more, you can specify its key file. The license period of your new license will be extended by 150 days as a bonus.

- Click **Specify** if you already have a serial number of your previous license. Enter its number and click **Next**.
- Click **Skip** if you don’t have a serial number of the previous license.

Frequently Asked Questions

How to transfer a license to another computer?

You can transfer your license using a key file or a serial number.

To transfer a license to another computer

- Using a serial number
  1. Uninstall Dr.Web from the computer of license origin or activate another license on this computer.
  2. Activate the current license on the target computer using a serial number. You can activate your license during the installation or during program operation.
- Using a key file
  1. Copy the key file from the computer of origin. By default, the key file is stored in the Dr.Web installation folder and has a `.key` extension.
  2. Uninstall Dr.Web from the computer of license origin or activate another license on this computer.
  3. Activate the current license on the target computer using a key file. You can activate your license during the installation or during program operation.

⚠ You cannot transfer a license for a trial period to another computer.

I forgot the registration email. How can I restore it?

If you forgot the address specified during registration, contact Doctor Web technical support.

If you make a request from an email address that differs from the one to which your license is registered, a technical support specialist may ask you to provide: a photo or a scan copy of the license certificate, payment receipt, an online store letter and other documents proving your license ownership.

How can I change the registration email?

If you want to change the email you specified during registration, use a special form on the Doctor Web website.

3.4. License Renewal

You can renew your current license in the **License Activation** section.

How can I renew the license if the license period hasn’t expired

1. In the Dr.Web menu , select **License**.
2. Click **Buy**. Complete your purchase on the Doctor Web website.

How can I renew the license if the license period has expired

1. In the Dr.Web menu , select **License**.
2. Click **Buy**. Complete your purchase on the Doctor Web website.

Dr.Web supports the update on the fly, thus you do not need to reinstall the program or interrupt its operation. To update Dr.Web license, activate a new license.

To activate your license

1. In the Dr.Web menu , select **License**.
2. Click **Activate**.
3. In the **License Activation** window,
   - Enter the serial number and click **Activate**.
   - If you have a key file, open the **Activation Files** tab. Drag the file to the dotted area or click to choose the file on your Mac.

The detailed information on license activation is available in the License Activation section.

If period of license you want to renew has expired, Dr.Web will use the new license.

If license you want to renew is still valid, the number of days remaining will be automatically added to the new license. At that, the previous license will be blocked. You will receive a notification on the email address you provided during registration.

3.5. License Restoration

If the key file is lost or corrupted, the operation of all Dr.Web components will be blocked and Mac security might be at risk. To reactivate the license, restore the key file using a serial number.

How to restore the key file

1. In the Dr.Web menu, select **License**.
2. Click **Activate**.
3. In the **License Activation** window, enter your serial number and click **Activate**.

When you reactivate your license, you receive the same key file.

How to restore the serial number

If you can't find your serial number, you can restore it in the following ways:

- Contact license seller (except for the boxed version).
- Use the recovery service on the Doctor Web website.
- Contact Doctor Web technical support. Attach to your request documents confirming that you are the owner of the license according to these rules.

You can reactivate the license, provided it has not expired.

You can activate the license with one serial number no more than 25 times. If this number is exceeded, contact Doctor Web technical support. Describe your problem in detail, specify the personal data you entered during registration and your serial number. You will get a license key file at the email you specified during registration.

3.6. Serial Number

Each license has a unique *serial number*. You can use it to activate the Dr.Web license.

Where can I find my Dr.Web serial number

If your serial number is not registered

- You can find your serial number in the email you received from the online store after you purchased your license.

- If you purchased your license in the Dr.Web online store via your Doctor Web account and registered your license in the loyalty program, your serial number will be stored in My purchases service.
- If you purchased your license in a box, you can find your serial number in the License certificate.

If your serial number is registered

- If Dr.Web is installed on your device, download this file and unpack it. Double-click on the `YSN.cmd` file. The `YourSerialNumber.txt` file will be created in the folder and automatically opened in the default text editor. All of your serial numbers will be listed in this file, after “SN =”.
- If Dr.Web is not installed on your device, restore the number using a service on the Doctor Web website.

If you are using Dr.Web on a subscription basis

In this case, you do not need a serial number or a key file.

- If you purchased your subscription on the Doctor Web website, you can find your subscription ID in My subscriptions section.
- If you purchased a subscription from a third-party provider, you can find the subscription ID in your account on the website of your IT service provider.

How to restore the serial number

If you can’t find your serial number, you can restore it in the following ways:

- Contact license seller (except for the boxed version).
- Use the recovery service on the Doctor Web website.
- Contact Doctor Web technical support. Attach to your request documents confirming that you are the owner of the license according to these rules.

3.7. Key File

The key file defines the license type and user rights for Dr.Web operation.

The license key file has the `.key` extension. You can receive the file during the license activation.

The key file contains the following information:

- The list of components licensed to the user
- Dr.Web license period
- Availability of technical support for the user

- Other restrictions (for example, the number of computers on which Dr.Web is allowed for operation).

> ⚠ The key file is located in the Dr.Web installation folder. The program regularly verifies the file. To avoid corruption of the key file, do not open it in text editors or try to modify it.
>
> If no valid key file is found, Dr.Web components are blocked.

A *valid* key file for Dr.Web satisfies the following criteria:

- License is not expired.
- Integrity of the key file is not violated.

If any of the conditions is violated, the key file gets *invalid*, and Dr.Web stops detecting and neutralizing malicious programs.

Keep the license key file until a license or a trial period expires. If you install Dr.Web on several computers or reinstall it, you can use the same license key file that you received during the first activation.

> ⚠ The key file for a trial period activation can be used only on the computer where the registration procedure was run.

4. Dashboard

On the **Dashboard** tab of the main window, you can:

- configure operation of protection components,
- scan your Mac for viruses,
- configure access parameters for your camera and microphone,
- update virus databases manually,
- view information on your current license,
- view information on detected threats.

Protection Components

- SpIDer Guard—file system monitor. Scans all files that users open in real time and monitors all programs and processes running on your Mac.
- SpIDer Gate—internet monitor. Scans HTTP traffic and monitors access to internet resources.
- Firewall—network monitor. Protects your Mac from unauthorized access and prevents data leaks via the network.

Scan Your Mac

Scanner—main component for virus detection with the following functions:

- Run express, full, and custom system scan on user demand.
- Neutralize detected threats (cure, delete, move to quarantine). You can choose the necessary action or specify automatic actions that will be applied to threats depending on their type.

Privacy Protection

- **Camera**—application access control to your camera.
- **Microphone**—application access control to your microphone.

Update

Click **Update Is Not Required/Update Is Required** to update virus databases manually. Virus databases contain information on all known malicious programs.

License

In the **License** section, you can view the information on your current license:

- status,
- number,
- owner,
- activation date,
- expiration date,
- number of remaining days.

You can activate the license if you already have a serial number, a key file, or a configuration file or buy a new license.

Threats

- Threats—common list of detected threats. You can delete, move to quarantine, or ignore the listed threats.
- Quarantine—a special folder which is used for isolation of infected files and other threats so that they cannot pose a threat to the system.

5. Notifications

On the **Notifications** tab, you can see the following notifications on the Dr.Web operation events:

- license status,
- threat detection and neutralization,
- virus databases status,
- errors in protection components operation,
- status of the central protection server connection,
- attempts to connect to your microphone or camera,
- messages from the central protection server administrator.

Dr.Web uses macOS system notifications to show messages on threat detection and neutralization or errors in component operation. You can disable or configure system notifications from Dr.Web.

To disable notifications

1. Choose the Apple menu > **System Preferences**
2. Select the **Notifications** section.
3. Select Dr.Web for macOS and disable notifications with switcher .

> ⚠ There is no switcher on macOS 10.14 and lower. To disable notifications, clear all checkboxes.

To configure system notifications

1. Choose the Apple menu > **System Preferences**.
2. Click **Notifications**.
3. In the left column, choose Dr.Web for macOS. Configure the program alert style and corresponding options.

6. Updating Virus Databases

In the **Updater** section, you can configure the frequency of virus databases update. Virus databases contain information on all known malicious programs.

New types of threats with more advanced disguise functions appear every day. Updating Dr.Web allows to detect previously unknown viruses, to block their spreading and sometimes to cure infected files which were incurable before.

> ⚠ Internet connection is required to update virus databases.

During the first launch, Dr.Web updates virus databases to the current state. Dr.Web then updates virus databases every 30 minutes. You can change the update frequency.

To change the frequency of virus databases update

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Updater** section.
3. Choose an update frequency from the **Update Virus Databases** drop-down list.

Dr.Web will automatically download updates according to the selected update frequency.

You can also start the update process manually.

To update virus databases manually

- In the main window, click **Update Is Not Required**/**Update Is Required**.

Dr.Web will check and update virus databases.

Proxy server configuration

If you do not want to install updates on your Mac directly, you can configure update installation via a proxy server.

To configure update installation via a proxy server

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Updater** section.

3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Select the **Use proxy server** check box.
5. Click **Configure proxy**.
6. Specify address and port of proxy server.
7. If proxy server requires password, select **Protect proxy server with a password** check box.
8. Specify your user name and password.
9. Click **Save**.

7. Real-Time File System Protection

The SpIDer Guard file system monitor scans all files that users open in real time and monitors all programs and processes running on your Mac.

You can exclude specific files and folders from real-time scanning.

SpIDer Guard is automatically enabled after you install and activate the Dr.Web license. The monitor launches at the system start and works constantly in the background.

When SpIDer Guard detects threats, it displays a warning and applies the action according to preferences. You can change actions that are automatically applied to various types of threats or apply actions manually.

To enable or disable SpIDer Guard

> ⚠ Only users with administrative privileges can disable SpIDer Guard.
>
> If real-time anti-virus protection is disabled, do not connect to the internet or open files from media that have not been scanned by Scanner.

To pause or continue real-time file system scan

1. On the **Dashboard** tab of the main window, choose **Protection Components**.
2. Enable or disable file system monitor SpIDer Guard by using the toggle .

SpIDer Guard doesn't work / System extension blocked

macOS 10.13 and later versions block kernel (system) extension loading. At that, SpIDer Guard doesn't work, and you see a notification saying that the system extension was blocked. For real-time file system scan to operate correctly, allow the loading of system software from Doctor Web Ltd.

To allow system extensions

1. Choose the Apple menu .
2. Click **System Preferences**.
3. Then choose the **Security & Privacy** section.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.

5. Click **Allow** next to the message about blocking the Doctor Web Ltd. system software.

> ⚠ The issue concerns users of macOS High Sierra 10.13 and later.

7.1. Configuring SpIDer Guard File Monitor

In the **SpIDer Guard** preferences section, you can specify actions that Dr.Web will automatically apply to threats depending on their type.

SpIDer Guard is designed to cure infected files, that are objects infected with known and potentially curable viruses. Suspicious objects and various types of malicious programs are moved to Quarantine.

You can change the actions that SpIDer Guard applies to each type of malicious objects. The list of available actions depends on the type of the threat:

Action	Description
Cure, move to quarantine if incurable	Restores the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within archives, email files, or file containers.
Cure, delete if incurable	Restores the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within archives, email files, or file containers.
Delete	Deletes the object. This action is not available for boot sectors.
Move to quarantine	Isolates the object in a special Quarantine folder. Protects you from the accidental loss of valuable data. This action is not available for boot sectors.
Ignore	Skips the object without performing any action or displaying a notification. This action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.

> Do not unnecessarily change default preferences of automatic actions.

To configure automatic actions

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Guard** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
4. If necessary, change automatic actions for the listed types of threats.

Advanced preferences

You can also configure SpIDer Guard and enable scanning of archives and emails and specify maximum time for scanning one object.

> Changing these preferences may slow down your Mac and increase the overall scanning time.

To enable scanning of archives and emails

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Guard** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
4. Click **Advanced**.
5. Select the **Archives** and **Email files** check boxes.
6. Click **Save**.

To specify maximum time for scanning one object

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Guard** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
4. Click **Advanced**.
5. Select the **Maximum time for scanning one object** check box.

6. Specify maximum time in seconds for scanning one object.
7. Click **Save**.

7.2. Excluding Files and Directories From Scanning

You can exclude specific files and folders from real-time scanning.

To exclude files and folders from scanning

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Exclusions** section.
3. Open the **Files and Folders** tab.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
5. Click the ⊞ button and select the necessary folder or simply drag the file to the list.
6. Click **Save**. Now SpIDer Guard will skip this file during scanning.

> If you want to scan the object without removing it from the exclusion list, clear the **SpIDer Guard** check box next to the object.

- To remove an object from the exclusion list, select it and click ⊟ or drag it outside the program window.
- To clear the exclusion list, select all the objects in the list (COMMAND-A) and click ⊟.

> The default exclusions preferences are optimal for most uses. Do not change them unnecessarily.
>
> ---
>
> By default, all quarantine folders are excluded from scans, because they are used to isolate detected threats and, as access to them is blocked, there is no use scanning these folders.

8. Web Traffic Scan

Every time browsers, download managers and applications connect to the internet, they exchange data with servers that host corresponding websites. SpIDer Gate internet monitor scans traffic and blocks transferring objects that may pose a threat to your Mac.

SpIDer Gate can also scan data transmitted via the secure HTTPS protocol. To configure encrypted traffic scan, enable the corresponding option in the Network section.

SpIDer Gate is automatically enabled after you install and activate the Dr.Web license. The monitor launches at the system start and works constantly in the background.

SpIDer Gate restrict access to non-recommended websites and webpages that violate copyright laws. You can change that by configuring access rules to specified websites and website categories.

You can also exclude specified websites and network connections of selected applications from the scan.

Enabling and disabling SpIDer Gate

> ⚠ Third-party applications for web traffic scan and web resources access control installed on your Mac may work incorrectly if SpIDer Gate is enabled.

To pause or continue web traffic scan

1. On the **Dashboard** tab of the main window, choose **Protection Components**.
2. Enable or disable SpIDer Gate by using the toggle .

SpIDer Gate doesn't work / System extension blocked

macOS 10.13 and later versions block kernel (system) extension loading. At that, SpIDer Gate doesn’t work, and you see a notification saying that the system extension was blocked. For web traffic scan to operate correctly, allow the loading of system software from Doctor Web Ltd.

To allow system extensions

1. Choose the Apple menu .
2. Click **System Preferences**.
3. Then choose the **Security & Privacy** section.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter

your user name and the password.

5. Click **Allow** next to the message about blocking the Doctor Web Ltd. system software.

> ⚠ The issue concerns users of macOS High Sierra 10.13 and later.

8.1. Configuring SpIDer Gate Internet Monitor

In the **SpIDer Gate** preferences section, you can configure parameters for network threats scanning and access to web resource.

SpIDer Gate restricts access to non-recommended websites and webpages that violate copyright laws. It also blocks suspicious programs, adware, and dialers.

You can configure scanning network threats, create access rules for specific webpages, and select additional website categories you want to restrict access to.

> ⚠ Do not unnecessarily change default preferences.

Threat scanning

On the **Threat Scanning** tab, you can specify parameters of network threats scanning, configure blocking of malicious program types, and specify maximum time for scanning one object.

SpIDer Gate restricts access to non-recommended websites and URLs listed due to a notice from copyright owners. Which websites does Dr.Web consider non-recommended?

You can remove access restrictions for these websites.

To remove restrictions

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Threat Scanning** tab, clear the **Block URLs listed due to a notice from copyright owners**, **Block non-recommended websites**, **Block not scanned objects** check boxes.

By default, Dr.Web skips objects that it failed to scan. You can enable scanning of such objects.

To enable blocking of unscanned objects

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Threat Scanning** tab, select the **Block not scanned content** check box.

By default, SpIDer Gate blocks suspicious programs, adware and dialers. You can configure blocking of malicious program types.

To configure blocking of malicious programs

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Threat Scanning** tab, select malware types to block.

You can specify maximum time for scanning one object.

> ⚠ Increasing the time for scanning one object may slow down your Mac.

To specify maximum time for scanning one object

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Threat Scanning** tab in **Maximum time for scanning one object** specify maximum time in seconds for scanning one object.

Website access

On the **Website Access** tab, you can specify access rules to specific websites and select website categories you want to temporarily restrict access to.

You can temporarily restrict access to website categories regardless of other SpIDer Gate preferences.

To restrict access to website categories

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Website Access** tab, select website categories you want to restrict access to:

Category	**Description**
Adult content	Websites that contain pornographic or erotic materials, dating sites, etc.
Violence	Websites that encourage violence or contain materials about various fatal accidents, etc.
Weapons	Websites that describe weapons and explosives or provide information on their manufacturing.
Gambling	Websites that provide access to online games of chance, casinos, auctions, including sites for placing bets, etc.
Drugs	Websites that promote use, production or distribution of drugs and so on.
Terrorism	Websites that contain aggressive and propaganda materials or terroristic attacks descriptions and so on.
Obscene language	Websites that contain the obscene language (in titles, articles and so on).
Chats	Websites that offer a real-time transmission of text messages.
Email	Websites that offer the possibility of free registration of an email box.
Social networks	Various social networking services: general, professional, corporate, interest-based; thematic dating websites.

You can temporarily restrict access to specific websites regardless of other SpIDer Gate preferences.

To restrict access to a specific website

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **SpIDer Gate** section.

3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. On the **Website Access** tab, click + under the table and enter the website address.

8.2. Excluding Websites From Scanning

You can exclude specific websites from web traffic scan. Access to these websites will be allowed regardless of the preferences of the SpIDer Gate internet monitor.

To allow access to a specific website

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Exclusions** section.
3. Open the **Websites** tab.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
5. Click + under the table and enter the website address.

- To remove an object from the exclusion list, select it and click − or drag it outside the program window.
- To clear the exclusion list, select all the objects in the list (COMMAND-A) and click −.

8.3. Encrypted Traffic Scan

Every time your Mac connects to the internet, it exchanges information with server that hosts a website. More and more web services turn to secure connections. They use a secure HTTPS protocol to transfer data. The exchange is secure because the SSL/TLS cryptographic protocol supports data encryption.

By default, Dr.Web does not scan encrypted traffic but you can enable that.

To enable encrypted traffic scan

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Network** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Enable the **Scan encrypted traffic** option.

For Dr.Web to scan encrypted traffic, website digital certificate gets replaced with Doctor Web security certificate.

What's a security certificate?

A security certificate is an electronic document that confirms that a certified program has been tested in one of certification centers.

A security certificate guarantees that connection is established in the protected mode with an authentication check.

When you install Dr.Web for macOS, Doctor Web security certificate is automatically imported in the list of system certificates. However, some applications, for example, browsers (Opera, Firefox) and mail clients (Mozilla Thunderbird, The Bat!), don't use system certificates as a reference.

For applications like that, you can export Doctor Web certificate manually and then install (import) it to the necessary application.

To export Doctor Web certificate

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Network** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Click **Export**.
5. Choose a folder where you want to save the certificate. Click **Save**.
6. Import the certificate to a target application. Find more details about the certificate import into target application’s user documentation.

⚠ If you have issues with cloud-based applications (for example, Google Drive, Dropbox, Yandex.Disk) after enabling the **Scan encrypted traffic** option, exclude them from the scan.

8.4. Excluding Applications From Scanning

You can exclude network connections of specified applications from being scanned. Connections for these applications will be allowed regardless of SpIDer Gate internet monitor preferences.

To exclude network connections of applications from being scanned

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Exclusions** section.
3. Open the **Applications** tab.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
5. Click the + and select the application or drag it to the list.

- To remove an object from the exclusion list, select it and click − or drag it outside the program window.
- To clear the exclusion list, select all objects in the list (COMMAND-A) and click −.

9. Protection From Network Threats

Firewall protects your Mac from unauthorized access and prevents leaks of important data. Firewall allows you to control application connections to the internet and data transfer via the network and block suspicious connections.

Firewall is automatically enabled after you install and activate the Dr.Web license. The monitor launches at the system start and works constantly in the background.

Firewall controls all incoming and outgoing traffic and allows or blocks application access to network resources according to the selected operation mode and specific filtering rules.

Enabling and disabling Firewall

> ⚠ Third-party applications for scanning web traffic and controlling access to web resources installed on your Mac may not work properly if Firewall is enabled.

To pause or continue protection from network threats

1. On the **Dashboard** tab of the main window, choose **Protection Components**.
2. Enable or disable Firewall by using the toggle .

Firewall doesn't work / System extension blocked

macOS 10.13 and later versions block kernel (system) extension loading. At that, Firewall doesn’t work, and you see a notification saying that the system extension was blocked. For protection from network threats to operate correctly, allow the loading of system software from Doctor Web Ltd.

To allow system extensions

1. Choose the Apple menu .
2. Click **System Preferences**.
3. Then choose the **Security & Privacy** section.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
5. Click **Allow** next to the message about blocking the Doctor Web Ltd. system software.

The issue concerns users of macOS High Sierra 10.13 and later.

Firewall blocked internet access

If an application (for example, a browser) can’t get access to the internet, create a new rule in the Firewall preferences.

9.1. Firewall Preferences

In the **Firewall** preferences section, you can specify parameters for scanning incoming and outgoing traffic and configure rules for specific applications to access internet resources.

Firewall allows access to network resources for all trusted applications. If application is not on the trusted list, Dr.Web displays a notification and asks which action to take.

Which applications are trusted by Dr.Web?

Among trusted applications are macOS system applications, applications with a security certificate or a valid digital signature. Rules for such applications are not displayed in the filtering list.

You can change Firewall operation mode and create filtering rules for specific applications that do not apply to selected operation mode.

Operation mode

Select one of the following operation modes:

- **Allow Trusted Applications**—access to network resources for all trusted applications is allowed (used by default). For other applications Dr.Web displays a notification and asks which action to take.
- **Allow All Connections**—access to network resources for all unknown applications is allowed. Known connections are processed by Firewall according to specified filtering rules.
- **Block All Connections**—access to network resources for all unknown applications is blocked. Known connections are processed by Firewall according to specified filtering rules.

To change the Firewall operation mode

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Firewall** section.

3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. At the top of the window, select the required operation mode from the drop-down list **Mode**.

Filtering rules

You can create filtering rules for specific applications. The specified rules are applied regardless of the selected Firewall operation mode.

A filtering rule includes:

- Application file in `.app` format.
- An action: to allow or to block the connection.
- A port number to connect to.
- An IP address, a website host name or a server host name that Firewall will control access to.

To create a new rule

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Firewall** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Click + under the table. A new rule window opens.
5. In the **Choose app** field, click ⌄.
6. Choose whether the rule applies to all applications or select an application on your Mac.
7. Choose **Block** or **Allow** from the drop-down list.
8. Specify the port number to connect to.

   ⚠ If you leave the **Port** field empty, rule will apply to all the ports.

   Exception: if you want to create a rule for all applications, you must specify the port number.

9. From the **Connection To** drop-down list, choose:
   - **Any Server** if you want to configure access to all servers and IP addresses.

   ⚠ If you want to create a rule for all ports, you must specify IP address or a host.

- **IP Address** if you want to configure access to a specific IP address. Enter an address in the IPv4 format: `192.0.2.235`.
- **Host** if you want to configure access to a specific host. Enter a website or a server host in the `example.com` format.

10. Click **Create**.

To edit the rule

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Firewall** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. In the filtering rules table, double-click the corresponding rule. The rule editing window opens.

> ⚠ If several rules are created for one application, click the ⌄ icon to expand the list.

5. Edit the necessary parameters of the rule.
6. Click **Save**.

10. Scanning Mac on Demand

Dr.Web Scanner scans objects in the file system on your demand and detects various threats that can hide themselves in the system. To protect your computer, it is necessary to periodically run a system scan with Dr.Web.

You can exclude specific files and folders from scanning on demand.

> ⚠ When your Mac is operating on battery power, the scanning is paused to prevent the battery from quick draining. Dr.Web displays a notification and let’s you decide to continue scanning or not. When you use a charge cable to power Mac, the scanning will be resumed automatically.

To run a quick scan of the most vulnerable parts of the system, select **Express Scan**. To perform a full scan of the file system, select **Full Scan**. You can also specify files and folders for scanning.

Scan types

Scan mode	Description
Express Scan	In this mode, the following objects are scanned: • Boot sectors of all disks • Random access memory • Boot disk root folder • System folder • Current user folder • Temporary files • System restore points • Presence of rootkits (if the process is run with administrative privileges) ⚠ Scanner does not check archives and email files in this mode.
Full Scan	Full scan of random access memory and all hard drives (including boot sectors of all disks), scan for rootkits.
Custom scan	Scan of any files or folders specified by the user

To run express scan

1. On the **Dashboard** tab of the main window, choose **Scan Your Mac**.

2. Click **Express Scan**.

To run full scan

1. On the **Dashboard** tab of the main window, choose **Scan Your Mac**.
2. Click **Full Scan**.

To run the scan of specific files and folders

1. On the **Dashboard** tab of the main window, choose **Scan Your Mac**.
2. Drag files and folders to the dotted area or click to choose the file or folder for scanning. Or drag files and folders to Dr.Web icon on the status bar.
3. Click **Scan**.

To run the scan of specific files and folders using the shortcut menu

1. Select a file or folder on the desktop or in the Finder.
2. Open the shortcut menu and select **Scan with Dr.Web**.

Scan results

Scan results are available if you

- interrupted the scanning (clicked **Stop**),
- Dr.Web has completed the scan of your Mac.

The scan results window displays:

- the number of scanned objects,
- the number of skipped objects,
- the number of detected threats,
- the number of neutralized threats.

When Scanner detects threats, it applies the action according to preferences. You can change actions that are automatically applied to various types of threats or apply actions manually.

To view detailed information on threats

- In the scan results window, click **Details**. The **Scan Details** tab opens.

On the **Scan Details** tab, you can see the detailed information on threats that Dr.Web detected during the last scan.

Why Dr.Web has skipped some objects

Reason	Solution
Insufficient privileges to apply action to the object.	Start scanning with administrative privileges.
The file size is too large.	Increase maximum time for scanning one object in Scanner preferences: Restart scanning.
The file is corrupted or password-protected.	If it is an archive, unpack it. Restart scanning.
There are archives in the list of skipped objects.	In the Scanner preferences, enable the **Archives** option or unpack the archives. Restart scanning.
There are email files in the list of skipped objects.	In the Scanner preferences, enable the **Email files** option or unpack the archives. Restart scanning.

Scanning with administrative privileges

To apply actions to some types of threats, Dr.Web may need administrative privileges.

To start scanning with administrative privileges

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Scanner** section.
3. Click **Advanced**.
4. Select **Start scanning with administrative privileges**.
5. Restart scanning.

10.1. Scanner Preferences

In the **Scanner** preferences section, you can specify actions that Dr.Web will apply to threats depending on their type.

Scanner is designed to cure infected files, that is objects infected with known and potentially curable viruses. Suspicious objects and various types of malicious programs are moved to Quarantine.

You can change the actions that Scanner applies to each type of malicious objects. The list of available actions depends on the type of the threat:

Action	Description
Cure, move to quarantine if incurable	Restores the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within archives, email files, or file containers.
Cure, delete if incurable	Restores the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within archives, email files, or file containers.
Delete	Deletes the object. This action is not available for boot sectors.
Move to quarantine	Isolates the object in a special Quarantine folder. Protects you from the accidental loss of valuable data. This action is not available for boot sectors.
Ignore	Skips the object without performing any action or displaying a notification. This action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.

⚠ You don’t have to enter your user name and the password to change the Scanner preferences. Preferences are automatically changed for all Mac users.

Do not unnecessarily change default preferences of automatic actions.

To configure automatic actions

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Scanner** section.

3. Enable the **Apply actions to threats automatically** option.
4. If necessary, change automatic actions for the listed types of threats.

Advanced preferences

Scanning with administrative privileges

To apply actions to some types of threats, Dr.Web may need administrative privileges.

To start scanning with administrative privileges

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Scanner** section.
3. Click **Advanced**.
4. Select **Start scanning with administrative privileges**.

Now Mac will ask for your user name and the password before each scan.

You can also configure scanning on demand and enable scanning of archives and emails and specify maximum time for scanning one object.

> ⚠ Changing these preferences may slow down your Mac and increase the overall scanning time.

To enable scanning of archives and emails

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Scanner** section.
3. Click **Advanced**.
4. Select the **Archives** and **Email files** check boxes.
5. Click **Save**.

> ⚠ Scanner does not scan archives and email files in the **Express Scan** mode.

To specify maximum time for scanning one object

1. In the main window, click ⚙.

2. In the **Preferences** window, select the **Scanner** section.
3. Click **Advanced**.
4. Select the **Maximum time for scanning one object** check box.
5. Specify maximum time in seconds for scanning one object.
6. Click **Save**.

Optimizing Mac battery life

When your Mac is operating on battery power, the scanning is paused to prevent the battery from quick draining. Dr.Web displays a notification and let's you decide to continue scanning or not. When you use a charge cable to power Mac, the scanning will be resumed automatically.

You can disable pausing the scanning when Mac switches to the battery mode.

To configure scanning while on battery power

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Scanner** section.
3. Click **Advanced**.
4. Disable (or enable) the **Pause scanning while on battery power** option.

10.2. Excluding Files and Directories From Scanning

You can exclude specific files and folders from scanning on demand.

To exclude files and folders from scanning

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Exclusions** section.
3. Open the **Files and Folders** tab.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
5. Click the + button and select the necessary folder or simply drag the file to the list.
6. Click **Save**. Now Scanner will skip this file during scanning on demand.

> ⚠ If you want to scan the object without removing it from the exclusion list, clear the **Scanner** check box next to the object.

- To remove an object from the exclusion list, select it and click − or drag it outside the program window.
- To clear the exclusion list, select all the objects in the list (COMMAND-A) and click −.

> The default exclusions preferences are optimal for most uses. Do not change them unnecessarily.
>
> ---
>
> By default, all quarantine folders are excluded from scans, because they are used to isolate detected threats and, as access to them is blocked, there is no use scanning these folders.

11. Privacy Protection

Dr.Web protects your privacy by controlling application access to the camera and microphone on your Mac.

By default, access to the camera and microphone is allowed for all applications. You can enable the camera and microphone access control.

> Camera and microphone access control is not available on macOS 10.14 or later.

To enable the camera and microphone access control

1. On the **Dashboard** tab of the main window, choose **Privacy Protection**.
2. Enable the camera and microphone access protection by using the toggle .

Every time an application tries to get access to your camera or microphone Dr.Web shows a notification and asks what action should be applied.

- **Block**—blocks access to your camera or microphone for the application. At that, access is blocked once. If the application tries to access your camera or microphone again, for example, if it is closed and started again, Dr.Web will display the notification again.
- **Allow**—allows access to your camera or microphone for the application.

  Users from the Administrators group have additional options for access control.

  - **Allow once**—allows access to your camera or microphone for the application once.
  - **Always allow**—always allows access to your camera or microphone for the application.

  If you choose the **Always allow** option, Dr.Web creates a separate rule for this application in the exclusion list.

> To create a rule in the exception list, you need administrator privileges.

11.1. Allow Access to Camera and Microphone

You can allow access to your camera and microphone to specific applications.

> Camera and microphone access preferences are not available on macOS 10.14 or later.

To allow access to your camera and microphone

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Exclusions** section.
3. Open the **Camera and Microphone** tab.
4. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
5. Click + under the **Camera** or **Microphone** lists, select necessary application and drag it to the corresponding list.

- To remove an object from the exclusion list, select it and click − or drag it outside the program window.
- To clear the exclusion list, select all objects in the list (COMMAND-A) and click −.

12. Neutralizing Threats

12.1. Threats

In the **Threats** section, you can view an overall list of threats and apply the necessary actions to them. To neutralize threats, configure automatic actions or apply actions to detected threats manually.

To view information on threats

1. On the **Dashboard** tab of the main window, choose **Threats**.

   On the **Threats** tab, all detected threats are displayed.

   In the status bar in the bottom of the window, the total number and the size of threats, and also the number and the size of selected threats are displayed.
2. To view the information on a certain threat, click the corresponding field.
3. If necessary, you can apply action to the threat. For that, select one of the following actions from the drop-down list:
   - **Delete** — completely remove the object from the file system.
   - **Move to quarantine** — move the object to quarantine.
   - **Ignore** — do not apply any actions.

To apply action to the threat

1. On the **Dashboard** tab of the main window, choose **Threats**.
2. Select one of the following actions for the corresponding threat from the drop-down list:
   - **Delete** — completely remove the object from the file system.
   - **Move to quarantine** — move the object to quarantine.
   - **Ignore** — do not apply any actions.
3. To neutralize all threats, click **Neutralize All**. This will apply actions specified in the program preferences for the corresponding types of threats.

⚠ If there are archives in the list of threats, action is applied to the whole archive.

If you want to apply the action to a specific file, unpack the archive and run scanning again.

To apply the action to several threats

1. Select several threats using the SHIFT key.

2. Use the following keyboard shortcuts:
   - COMMAND-SHIFT-D — delete threats.
   - COMMAND-SHIFT-M — move threats to quarantine.

12.2. Quarantine

In the **Quarantine** section, you can view information and apply actions to objects stored in quarantine. Quarantine is a special folder that allows isolating detected threats from the rest of the system if the object is incurable, but you want to keep it.

> Due to the privacy reasons, the quarantine folder is created for each user in the system. Therefore, if you switched to the administrator mode, the detected threats which are moved to the administrator quarantine and will not be available in the user quarantine folders.

To view information on the objects in quarantine

1. On the **Dashboard** tab of the main window, choose **Threats**.
2. Open the **Quarantine** tab.
3. To view the information on a certain object in quarantine, double-click the corresponding field.

To apply the action to the object in quarantine

1. On the **Dashboard** tab of the main window, choose **Threats**.
2. Open the **Quarantine** tab.
3. Select one of the following actions for the corresponding object from the drop-down list:
   - **Delete** — completely remove the object from the file system.
   - **Restore** — return the object to the initial folder.
   - **Restore To** — select the folder to restore the object to.

> Objects in quarantine can not be cured. You can scan the object again if you doubt that the file is malicious.
>
> You can also restore the object. Curing algorithms are being constantly improved. The object might be cured after the next program update.

> If there are archives in the list of threats, action is applied to the whole archive.

If you want to apply the action to a specific file, unpack the archive and run scanning again.

To apply the action to several threats

1. Select several threats using the SHIFT key.
2. Use the following keyboard shortcuts:
   - COMMAND-SHIFT-D — delete the threat.
   - COMMAND-SHIFT-R — return the object to the initial folder.
   - COMMAND-SHIFT-P — select the folder to restore the object to.

13. Support

13.1. Help

To open Dr.Web help

1. In the main window, click .
2. Select the **Help** tab.

If you cannot find a solution for your problem in the help, check out the list of questions and answers. If you’re not managed to find the answer, contact Doctor Web technical support.

13.2. Questions and Answers

Below are some possible issues that you may encounter when using Dr.Web with explanations on why they may occur and suggestions on how to deal with them. Please read this topic before contacting technical support.

General issues

The SpIDer Gate, SpIDer Guard, and Firewall components are disabled

macOS blocks kernel (system) extension loading. For SpIDer Gate and SpIDer Guard to operate correctly, allow loading of system software from Doctor Web Ltd. in the Security & Privacy System Preferences pane.

1. Choose the Apple menu .
2. Click **System Preferences**.
3. Then choose the **Security & Privacy** section.
4. If preferences are unavailable, unlock them. To do that, click at the bottom and enter your user name and the password.
5. Click **Allow** next to the message about blocking the Doctor Web Ltd. system software.

> The issue concerns users of macOS High Sierra 10.13 and later.

I have a license, but Dr.Web does not work

- Make sure that your license period hasn't expired. To check the license period and buy a new license, go to the **License** section of Dr.Web main window.
- You may have upgraded the operating system and installed version of Dr.Web does not support the new version of macOS. Uninstall the current version of Dr.Web and reinstall the program.

Dr.Web hangs up or lags

This may be caused by high activity of system processes which consume a lot of memory resources. Close unused apps to free up some memory. You can view the information and manage running processes with macOS standard tool Activity monitor.

If the issue persists, try reinstalling the program.

Firewall blocked internet access

Create a new rule for the application that can't get access to the internet in the Firewall preferences.

There are no sound alerts although they are enabled

Check the sound volume in System Preferences and on speakers.

Preferences are blocked

Preferences of some components are protected. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.

Scanning issues

File system scanning does not work (cannot run Scanner or enable SpIDer Guard)

Make sure that your license period hasn't expired. To check the license period and buy a new license, go to the **License** section of Dr.Web main window.

Dr.Web virus databases take a lot of time to load or the scanning is very slow

- Dr.Web loads virus databases every time it starts scanning or attempts to cure an object. Thus, these operations may take some time.
- Hang-ups and lags may also be caused by high activity of system processes which consume a lot of memory resources. We recommend you to close unused apps to free up some memory. You can find more information and manage running processes in macOS standard tool Activity monitor.

Some files are skipped during scanning

- Files (or folders in which they are contained) may be excluded from the scan.
- Some files may be skipped during scanning because they are corrupted or password-protected or you need administrative privileges to access files. If there are archives in the list of skipped objects, try to unpack them before scanning.

Scanner hangs up

If Scanner hangs up, try closing and restarting the app. If the issue persists, try reinstalling the program.

SpIDer Gate operation issues

SpIDer Gate does not block websites from selected categories

- Make sure that the corresponding category check box is selected on the SpIDer Gate tab.
- If connection to a website was established before SpIDer Gate was enabled, disable and enable SpIDer Gate and restart the browser.
- Check if website uses a secure connection (in this case, lock appears in the browser address bar). If secure connection is used, select **Scan encrypted traffic** check box on the Network tab and restart the browser.
- SpIDer Gate does not block websites which use connection via FTP/SPDY or HTTP/2.0.

Certificate error message appears when opening the website

- The error may occur because some browsers or mail clients do not refer to the system certificate storage while sending and receiving encrypted traffic. In this case, install Doctor Web certificate which you can obtain by clicking Export button on the Network tab.

- If browser or mail client was launched directly after installation, it might not obtain the system security certificate. In this case, you need to restart your browser or mail client.
- Original server certificate may be untrusted. To check it, disable SpIDer Gate and restart your browser or mail client. If error persists, it means that certificate is untrusted and it is not recommended to visit this website.

SpIDer Gate has blocked the website you need to visit

This website is probably included in the blocked category of websites. To access the website, add it to exclusions.

Update

Update is not loaded

- Check your internet connection.
- If you are using a proxy server, try turning it off and running an update again. To run update manually, in Dr.Web menu select **Update Is Required**.
- If router is working in the Connection on demand mode, make sure that connection is constantly active (maximum idle time is 0).
- Make sure that your license period hasn't expired. To check the license period and buy a new license, go to the **License** section of Dr.Web main window.

License

Trial period has not expired, but license is invalid

- License for the trial version is tied to a checksum of the operating system. You may have upgraded the operating system or other software or replaced computer components and checksum has changed.
- License for the trial version is tied to the MAC address of your device. You may have changed the MAC address and license has become invalid.

Contact Doctor Web technical support or activate new trial version using another email address.

Unable to activate the license

- Check your internet connection.

- If you are using a proxy server, try turning it off and running an update again. To run the update manually, in Dr.Web menu, select **Update Is Required**.
- If router is working in the Connection on demand mode, make sure that connection is constantly active (maximum idle time is 0).

If you have issues with Doctor Web operation that are not described above, contact Doctor Web technical support. For Doctor Web specialists to help you as quickly as possible, try to give as much information as possible about the problem.

13.3. Error Codes

Code	Error	Description
1	Error on monitor channel	One of the components cannot connect with the configuration daemon Dr.Web ConfigD.
2	Operation is already in progress	Operation requested by the user is already in progress.
3	Operation is in pending state	Operation requested by the user is in pending state (probably, a network connection is currently establishing or one of the program components is loading or initializing, which takes a long time).
4	Interrupted by user	Action is terminated by the user (probably, action took too much time).
5	Operation canceled	Action is cancelled (probably, action took too much time).
6	IPC connection terminated	Inter-process communication (IPC) connection with one of the components is terminated (most likely, component shuts down because of the user command or being idle).
7	Invalid IPC message size	Message of invalid size is received during component inter-process communication (IPC).
8	Invalid IPC message format	Message of invalid format is received during component inter-process communication (IPC).
9	Not ready	Required action cannot be performed because the necessary component or device is not initialized yet.
10	The component is not installed	Some function of Dr.Web for macOS is not available because the corresponding component (performing this function) is not installed in the system.
11	Unexpected IPC message	Unexpected message is received during component inter-process communication (IPC).

12	IPC protocol violation	Protocol violation happens during component inter-process communication (IPC).
13	Subsystem state is unknown	Current state is not known for a certain subsystem that is a part of this software and is needed for carrying out the requested operation.
20	Path must be absolute	Absolute path to file or directory is required (beginning with root directory of the file system). Relative path is used now.
21	Not enough memory	Not enough memory to complete the required operation (for example, an attempt to open a large file).
22	IO error	An input/output (I/O) error has occurred (for example, the drive is not initialized yet or the partition of the file system is not available anymore).
23	No such file or directory	Specified object of the file system (file or directory) is missing. It is probably removed.
24	Access denied	Insufficient rights to access specified object of the file system (file or directory).
25	Not a directory	Specified object of the file system is not a directory. Enter the path to the directory.
26	Data file corrupted	Requested data is corrupted.
27	File already exists	On attempt to create a file, another file with the same name is detected.
28	Read-only file system	On attempt to create or change an object of the file system (directory, file, or socket), it is detected that the file system is read-only.
29	Network error	Network error occurs (probably, a remote host stopped responding unexpectedly or the required connection fails).
30	Not a drive	Accessed input/output (I/O) device is not a drive.
31	Unexpected EOF	During data reading, the end of the file is reached unexpectedly.
32	File was changed	During scanning the file, it is detected that the file was changed.
33	Not a regular file	During accessing an object of the file system. it is detected that it is not a regular file (that is, it is a directory, socket, or other object of the file system).
34	Name already in use	On attempt to create an object of the file system (directory, file, or socket), another object with the same name is detected.

35	Host is offline	Remote host is not available through the network.
36	Resource limit reached	The limit defined for the use of a certain resource has been reached.
37	Different mount points	Attempt to restore a file which requires its movement between the file system directories, which belong to different mounting points.
38	Unpacking error	Archive unpacking unsuccessful (it is probably password protected or corrupted).
40	Virus database corrupted	It is detected that virus databases are corrupted.
41	Non-supported virus database version	It is detected that current virus databases are meant for earlier program version.
42	Empty virus database	Virus databases are empty.
43	Object cannot be cured	An attempt to apply the **Cure** action to an incurable object during threat neutralization.
44	Non-supported virus database combination	Used virus database combination cannot be supported.
45	Scan limit reached	When scanning an object, the specified limits have been reached (for example, the limit on the size of an unpacked file, on the nesting depth, and so on).
47	Authentication failed	Invalid user credentials are used for authentication.
48	Authorization failed	A user whose credentials are used for authorization does not have enough privileges.
49	Access token is invalid	One of the program components provides an invalid authorization token on attempt to access the operation requiring elevated privileges.
60	Invalid argument	An invalid argument is used on attempt to run a command.
61	Invalid operation	An attempt to run an invalid command is detected.
62	Root privileges required	Only a user with root privileges can perform this action.
63	Not allowed in central protection mode	The required action can be performed only if the program operates in the standalone mode.
64	Non-supported OS	The program does not support operating system installed on the host.
65	Feature not implemented	Required features of one of the components are not implemented in the current version of the program.

66	Unknown option	The configuration file contains parameters unknown or non-supported in the current version of the program.
67	Unknown section	The configuration file contains sections unknown or non-supported in the current version of the program.
68	Invalid option value	One of the parameters in the configuration file contains an invalid value for the parameter.
69	Invalid state	The program or one of the components is in an invalid state to complete the required operation.
70	Only one value allowed	One of the parameters in the configuration file contains a list of values; while it is allowed to contain only a single value.
71	Tag value is invalid	One of the sections in the configuration file with a name containing a unique tag identifier has an invalid tag identifier.
80	Record not found	On attempt to access a threat record, it is detected that the record is missing (probably, another program component processed the threat).
81	Record is in process now	On attempt to access a threat record, it is found out that another program component is processing the record now.
82	File has already been quarantined	On attempt to move the file with the detected threat to quarantine, it is detected that the file is already in quarantine (most likely, another program component processed the threat).
89	Cannot backup before update	Prior to downloading the updates from the update server, an attempt to make a backup copy of the files to be updated failed.
90	Invalid DRL file	An integrity violation of one of the files with the list of update servers is detected.
91	Invalid LST file	An integrity violation of the file containing the list of updated virus databases is detected.
92	Invalid compressed file	An integrity violation of the downloaded file containing updates is detected.
93	Proxy authentication error	Program fails to connect to update servers using the proxy server specified in preferences.
94	No update servers available	Program fails to connect to any of update servers.
95	Invalid key file format	Key file format is violated.
96	License is expired	Current license is expired.
97	Network operation timed out	Network operation timed out.

98	Invalid checksum	Checksum of downloaded file containing updates is invalid.
99	Invalid demo key file	Used demo key file is invalid (for example, it was received from another computer).
100	License key file is blocked	Used license is blocked (probably, the license agreement conditions on using the Dr.Web program are broken).
101	Invalid license	Used license is meant for other product or does not allow operation of the installed product components.
102	Invalid configuration	One of the program components cannot be in operation because of incorrect configuration preferences.
104	Invalid executable file	One of the program components cannot run due to incorrect path or corrupted execution file contents.
105	Virus-Finding Engine is not available	A file of Dr.Web Virus-Finding Engine is missing or unavailable (it is necessary for threat detection).
106	No virus databases	Virus databases are missing.
107	Process terminated by signal	A component shuts down (probably, because of the user command or being idle).
108	Unexpected process termination	A component unexpectedly shuts down because of a failure.
109	Incompatible software detected	A program component cannot be in operation because an incompatible software is detected. This software interrupts correct component operation.
110	Invalid VadeRetro library	A file of VadeRetro anti-spam library is missing, unavailable or corrupted. It is necessary for email scanning.
112	Databases of web resource categories	Databases of web resource categories are missing.
113	Kernel module for SpIDer Guard is not available	The kernel module required for SpIDer Guard operation is missing.
117	SpIDer Gate is not available	SpIDer Gate component required for scanning network connections is missing.
118	MailD is not available	SpIDer Mail component required for scanning email is missing.
119	Scanning Engine is not available	Cannot scan files as Scanning Engine component is missing or failed to start. This module is used for searching malicious objects.
120	Scanner is not available	Cannot scan files as Scanner component used for this function is missing.

121	ESAgent is not available	ESAgent component is missing. The component is necessary for connection to the central protection server.
122	Firewall is not available	Cannot control network connections as Firewall component is missing or failed to start. The module is used to divert connections.
123	Network Checker is not available	Cannot control network connections as Network Checker component is missing or failed to start. The module is used to scan the downloaded files.
124	CloudD is not available	The CloudD component required for connection to Dr.Web Cloud service is missing.
125	Unexpected error	Unexpected error occurs in operation of one of the components.

13.4. 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.

14. General Preferences

In the **General** section, you can configure sound alerts, on-screen notifications, choose program language, and restore default preferences.

> ⚠ You don’t have to enter your user name and the password to change general preferences. Preferences are automatically changed for all Mac users.

Notifications

Dr.Web uses macOS system notifications to show messages on threat detection and neutralization or errors in component operation.

To disable notifications

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **General** section.
3. Clear the **Enable notifications** check box.

Sound alerts

Dr.Web uses sound alerts to notify you about threat detection, neutralization, and deletion.

To disable sound alerts

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **General** section.
3. Clear the **Use sound alerts** check box.

Restoring default preferences

If you experience any difficulties with Dr.Web operation after changing program preferences, you can restore defaults. At that, all your changes of preferences will be lost.

To restore default preferences

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **General** section.

3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and the password.
4. Click **Restore Defaults**.
5. Click **Restore** to confirm restoring default program preferences.

15. Connection to Cloud Services

Dr.Web connects to cloud services to protect your Mac from the latest threats and improve operation of program components. Cloud services provide users with protection from infected files and restrict access to unwanted websites.

Depending on virus database update preferences, information on threats can be out of date. Data is processed faster with cloud services than local virus databases are updated on the computer.

Also, impersonal data about Dr.Web component operation is automatically sent to Doctor Web servers. You can read the privacy policy statement on Doctor Web official website ↗.

To disconnect from cloud services

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Dr.Web Cloud** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Disable the **I want to connect to services (recommended)** option.

16. Central Protection Mode

Centralized protection of your Mac is provided by Dr.Web Enterprise Security Suite server administrator or by your IT provider via Dr.Web AV-Desk anti-virus service. Your personal license is not used in the central protection mode.

Preferences and components

Dr.Web preferences and component operation can be modified and blocked in compliance with company security policy or according to the list of purchased services of your provider. The following preferences and components can be controlled from the server:

- Virus databases update. Updates are downloaded automatically from the central protection server. If the server connection is unavailable, updates are downloaded via the internet from Dr.Web servers.
- Real-time file system protection
- Web traffic scan
- Scanning Mac for viruses. Anti-virus network administrator can run remote scanning of your Mac manually or according to the schedule.

Connecting Mac

Every Mac with an installed Dr.Web is a separate station. Depending on the authorization preferences of the central protection server, station can be connected to the anti-virus network in one of the following modes:

- Automatically if the station has already been created on the server and it has an ID and a password.
- As a newbie. Dr.Web creates a new ID and a password. In this case, an approval on the server may be required or a station may be automatically authorized depending on the access preferences on the server.

> ⚠ For detailed information on connecting a station to the server, refer to the Dr.Web Enterprise Security Suite and Dr.Web AV-Desk administrator manuals.

Automatic connection

If you’ve bought subscription to the Dr.Web AV-Desk anti-virus service, you can install Dr.Web using the file in `.cdr` format that contains parameters for connection to the server. To get the `.cdr` file, contact your IT provider.

To install Dr.Web using the .cdr file

1. Run the file you received.
2. Click **Install Dr.Web**.
3. Accept the terms of the License Agreement. The installation process starts.
4. Enter administrator password and click **Install Helper**.
5. Dr.Web for macOS will be copied into the **Applications** folder and start automatically.

Connection to the central protection server will be automatically configured.

If anti-virus network administrator of your company or IT provider provided you with a configuration file in `.cfg` format, you can connect Dr.Web in the **License Activation** section. Parameters required for connection to the central protection server will be automatically configured.

To connect the station using the .cfg file

1. In the main Dr.Web window, select **License**.
2. Click **Activate**.
3. In the **License Activation** window, open the **Activation Files** tab.
4. Drag the `.cfg` file to the dotted area or click to choose the file on your Mac.
5. Once the activation is completed, parameters required for the server connection are automatically configured.

If anti-virus network administrator of your company provided you with a certificate or with a public encryption key in `.pub` format, you can configure connection parameters manually.

To configure server connection parameters manually

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Mode** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Set the **Enable central protection mode** check box. Once the central protection mode is enabled, parameters of the last connection are restored.
5. Specify server IP address and port number required for the server connection.
6. Drag a certificate or a public encryption key file in `.pub` format to the dotted area or double-click to choose the file on your Mac.

7. Expand the **Authentication** subsection.
8. Disable **Connect as a newbie station** option. Specify additional parameters for workstation authorization.
   - Station ID
   - Password (assigned to your computer for registration on the server)
   - Traffic compression mode
   - Traffic encryption mode

   The entered values are saved using the Keychain system. Therefore, you don’t need to enter them again when reconnecting to the server.
9. Click **Connect**.

Connecting the station as a newbie

If administrator hasn’t created a station on the server yet, you can connect it as a newbie. Contact anti-virus network administrator of your company or IT provider to get a certificate or a public encryption key and parameters for connection to the central protection server.

To connect the station as a newbie

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Mode** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Set the **Enable central protection mode** check box.
5. Specify server IP address and port number required for the server connection.
6. Drag a certificate or a public encryption key file in `.pub` format to the dotted area or double-click to choose the file on your Mac.
7. Make sure that the **Connect as a newbie station** option is enabled in the **Authentication** subsection.
8. Click **Connect**.

Standalone mode

You can disable the central protection mode and restore autonomous operation of Dr.Web.

When switching to this mode, all program preferences are restored to their previous or default states. You can once again access all Dr.Web components.

For correct operation in the standalone mode, Dr.Web requires a valid personal license key file. License received from the central protection server cannot be used in this mode. If necessary, activate your personal license.

To return to the standalone mode

1. In the main window, click ⚙.
2. In the **Preferences** window, select the **Mode** section.
3. If preferences are unavailable, unlock them. To do that, click 🔒 at the bottom and enter your user name and password.
4. Clear the **Enable central protection mode** check box.
5. Click **Disable** to confirm the action.

17. Reference Information

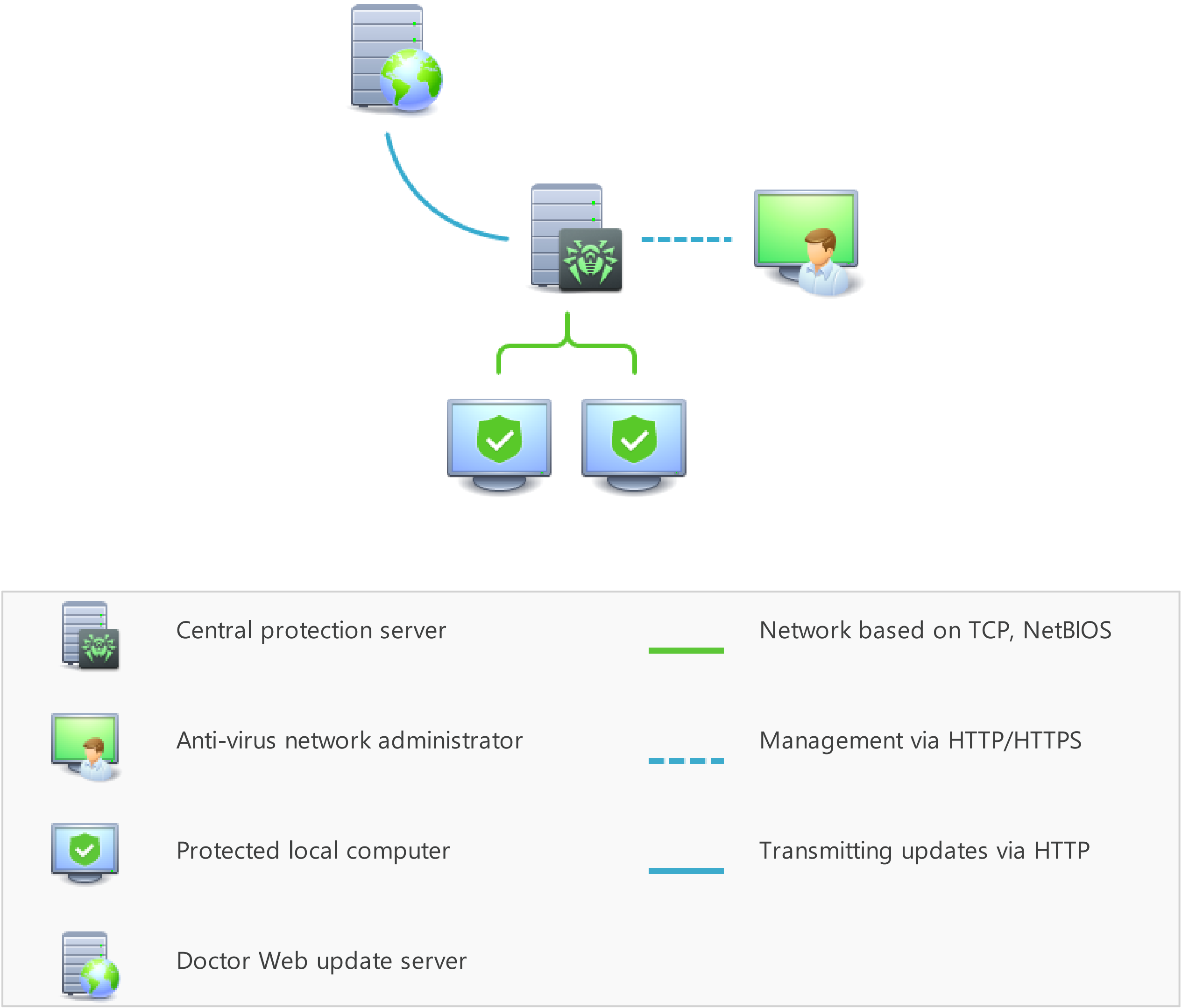
17.1. Central Protection and Anti-Virus Network

Solutions for central protection from Doctor Web help automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one *anti-virus network* which security is monitored and managed from central server by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

Doctor Web solutions for central protection use client-server model (see the figure below).

Local *anti-virus components* (clients, in that case, Dr.Web for macOS) protect computers of the company or users of IT service provider. Anti-virus components provide protection and ensure easy connection to the central protection server.


Central protection server
Anti-virus network administrator
Protected local computer
Doctor Web update server
Network based on TCP, NetBIOS
Management via HTTP/HTTPS
Transmitting updates via HTTP

Picture 1. Logical structure of the anti-virus network

Local computers are updated and configured via the *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from Dr.Web update servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.

⚠ Local anti-virus components are not compatible with other anti-virus software including versions of Dr.Web anti-virus solutions that do not support operation in the central protection mode (i.e. Dr.Web version 5.0). Installing two anti-virus apps on one computer may lead to system crash and loss of important data.

Central protection solutions

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite is a complex solution for corporate networks of any size that provides reliable protection of workstations, mail and file servers from all types of modern computer threats. This solution also provides diverse tools for anti-virus network administrators that allow them to keep track and manage operation of local anti-virus components including components deployment and update, network status monitoring, statistics gathering, and notification on virus events.

Dr.Web AV-Desk internet service

Dr.Web AV-Desk is an innovative Internet service created by Doctor Web for providers of various types of Internet services. With this solution, providers can deliver information security services to home customers and companies providing them with a selected package of services for protection from viruses, spam and other types of computer threats for as long as is necessary. Services are provided online.

For more information on Dr.Web AV-Desk internet service, visit the official Doctor Web website at https://www.av-desk.com/.

17.2. Threat Types

Herein, the term *“threat”* is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user’s information or rights (that is, malicious and other unwanted software). In a wider sense, the term “threat” may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger user data or confidentiality. Programs that do not conceal their presence in the system (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

Computer Viruses

This type of computer threats is characterized by their ability to inject malicious code into running processes of other programs. This action is called *infection*. In most cases, the infected file becomes a virus carrier itself, and the injected code does not necessarily match the original one. The majority of viruses are created with a purpose to damage or destroy data in the system.

Doctor Web divides viruses by the type of objects they infect into the following categories:

- *File viruses* infect files of the operating system (usually executable files and dynamic libraries) and are activated when the infected file is launched.
- *Macro-viruses* are viruses that infect documents used by **Microsoft® Office** and some other applications supporting macro commands (for example, written in **Visual Basic**). *Macro commands* are a type of implemented programs (macros) written in a fully functional programming language. For instance, in **Microsoft® Word**, macros can be automatically initiated upon opening (closing, saving, and so on) a document.
- *Script viruses* are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and, thus, take advantage of script vulnerabilities in web applications.
- *Boot viruses* infect boot records of disks and partitions or master boot records of hard drives. They do not require much memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down is performed.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved, and ways to overcome them are constantly being developed. All viruses may also be classified according to protection type they use:

- *Encrypted viruses* encrypt their code upon every infection to hinder their detection in a file, a boot sector or a memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.
- *Polymorphic viruses* nit only encrypt there code, but they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.
- *Stealth viruses* (invisible viruses) perform certain actions to disguise their activity and to conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these “dummy” characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, and others) or according to affected operating systems.

Computer Worms

Recently, malicious programs of the “computer worm” type have become much more common than viruses and other types of malware. Just like viruses, such programs can make copies of themselves, however they do not infect other objects. A worm gets into a computer from a network (most frequently as an attachment to an email or from the Internet) and sends the functioning copies of itself to other computers. To start their spread, worms can either rely on the computer user’s actions or can select and attack computers in an automatic mode.

Worms do not necessarily consist of only one file (the worm’s body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm’s body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm’s body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

Doctor Web classifies worms in accordance with their distribution methods as follows:

- *Network worms* spread via various network and file-sharing protocols.
- *Mail worms* spread themselves using email protocols (POP3, SMTP, etc.)
- *Chat worms* use protocols of popular instant messengers and chat programs (ICQ, IM, IRC, etc.)

Trojan Programs (Trojans)

These programs cannot replicate themselves. Trojans substitute a frequently-used program and perform its functions (or imitate its operation). Meanwhile, they perform some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or make it possible for hackers to access the computer without permission, for example, to harm the computer of a third party.

Like viruses, these programs can perform various malicious activities, hide their presence from the user, and even be a virus component. However, usually, Trojans are distributed as separate executable files (through file-exchange servers, data carriers, or email attachments) that are run by users themselves or by some specific system process.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are attributed to Trojans only. Here are some Trojan types which are distinguished as separate classes in Doctor Web:

- *Backdoors* are Trojans that log on into the system and obtain privileged functions, bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.

- *Rootkits* are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: *User Mode Rootkits (UMR)* that operate in user mode (intercept functions of the user mode libraries) and *Kernel Mode Rootkits (KMR)* that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).
- *Keyloggers* are used to log data that users enter by means of a keyboard in order to steal personal information (i.e. network passwords, logins, credit card data, etc.).
- *Clickers* redirect hyperlinks to certain addresses (sometimes malicious) in order to increase traffic of websites or perform DDoS attacks.
- *Proxy Trojans* provide anonymous Internet access through a victim’s computer.

In addition, Trojans can also change the start page in a web browser or delete certain files. However, these actions can also be performed by other types of threats (viruses and worms).

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in web browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These software applications were not created for malicious purposes, but due to their characteristics can pose a threat to the computer’s security. Riskware programs can not only damage or delete data, but they are also used by crackers (i.e. malevolent hackers) or by some malicious programs to harm the system. Among such programs, there are various remote chat and administrative tools, FTP-servers, etc.

Suspicious objects

These are potential computer threats detected by the heuristic analyzer. Such objects can be any type of threat (even unknown to information security specialists) or turn out safe in case of a false detection. It is strongly recommended to move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.

17.3. Detection Methods

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which allows them to perform thorough checks on suspicious files and control software behavior.

Signature analysis

The scans begin with signature analysis that is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

On completion of signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing method to detect new and modified viruses that use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing mechanism allows to considerably reduce the number of false triggering of the heuristic analyzer. Objects detected using the Origins Tracing algorithm are indicated with the `.Origin` extension added to their names.

Execution Emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses when a search by checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator*—a programming model of the processor and runtime environment. An emulator operates with protected memory area *(emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus code, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristic analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) that might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristic analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristic analyzer also uses the FLY-CODE technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers Dr.Web is aware of, but also by new, previously unexplored programs. While checking packed objects, Dr.Web anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (omit viruses or raise false positives). Thus, objects detected by the heuristics analyzer are treated as “suspicious”.

Behavior Analysis

Dr.Web Process Heuristic

The Dr.Web Process Heuristic behavioral analysis technology protects systems against new dangerous malicious programs that can avoid detection by traditional signature-based and heuristic analyses.

Dr.Web Process Heuristic analyses the behavior of each running program in real time. Using the constantly updated Dr.Web cloud service, along with the information on malware behavior, it determines whether the program is dangerous and then takes necessary measures to neutralize the threat.

This data protection technology helps to minimize losses resulting from the actions of unknown malware while consuming very few of the protected system's resources.

Dr.Web Process Heuristic monitors any attempts to modify the system:

- Detects malicious processes that modify users' files (such as actions of encryption ransomware).
- Prevents malware from injecting its code into the processes of other applications.
- Protects critical system areas from being modified by malware.
- Detects and shuts down the execution of malicious, suspicious or unreliable scripts and processes.
- Prevents malware from modifying boot sectors so that malicious code cannot be executed on the computer.
- Blocks changes in the Windows Registry to make sure that the safe mode won't be disabled.
- Prevents malware from changing launch permissions.
- Prevents new or unknown drivers from being downloaded without the user's consent.
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries into the Windows Registry, so that they could be launched automatically.
- Locks registry sections containing information about virtual device drivers, ensuring that no new virtual devices are created.
- Prevents malware from disrupting system routines such as scheduled backups.

Dr.Web Process Dumper

Dr.Web Process Dumper, a comprehensive analysis of packed threats significantly improves the detection of supposedly "new" malicious programs that were added to the Dr.Web virus database before they were concealed by new packers. In addition, this type of analysis eliminates the need to keep adding new entries into the virus database. With Dr.Web virus databases kept small, system requirements do not need to be constantly increased. Updates remain traditionally small, while the quality of detection and curing remains at the same traditionally high level.

Machine learning

Machine learning is used for detecting and neutralizing malicious objects missing from the virus databases. The advantage of the method is detection of a malicious code without executing it, judging only by its features.

Threat detection is based on the malicious object classification according to specific features. Support vector machines (SVM) underlie machine learning technologies that are used for classification and adding code fragments written in scripting languages to the databases. Detected objects are then analyzed on the basis of whether they have features of a malicious code. Machine learning technology makes the process of updating these features and virus databases automatic. Large amounts of data are processed faster thanks to the connection to the cloud service, and continuous training of the system provides preventive protection from the latest threats. At that, the technology can function even without a constant connection to the cloud.

The machine learning method significantly saves the resources of the operating system, since it does not require code execution to detect threats, and dynamic machine learning of the classifier can be carried out without a constant update of the virus databases that is used for signature analysis.

Cloud-based threat detection technologies

Cloud-based detection methods allow to scan any object (file, application, browser extension, etc.) by its hash value. Hash is a unique sequence of numbers and letters of a given length. When analyzed by a hash value, objects are scanned using the existing database and then classified into categories: clean, suspicious, malicious, etc.

This technology optimizes the time of file scanning and saves device resources. The decision on whether the object is malicious is made almost instantly, because it is not the object that is analyzed, but its unique hash value. If there is no connection to the Dr.Web servers, the files are scanned locally, and the cloud scan resumes when the connection is restored.

Thus, the Doctor Web cloud service collects information from numerous users and quickly updates data on previously unknown threats increasing the effectiveness of device protection.

17.4. Keyboard Shortcuts

You can use special keyboard combinations to start system scanning, to apply actions to detected threats or to configure Dr.Web.

Combination		**Action**
Actions for detected threats	COMMAND-SHIFT-C	Cure the threat
	COMMAND-SHIFT-M	Move the threat to quarantine
	COMMAND-SHIFT-I	Ignore the threat
	COMMAND-SHIFT-D	Delete the threat
	COMMAND-SHIFT-R	Restore the threat
	COMMAND-SHIFT-P	Choose the folder, where you want to restore the threat

Combination		Action
General	COMMAND-A	Select all
	COMMAND-W	Close