Dr.WEB

Security Space (macOS)

User Manual

Dr.Web Security Space (macOS)
Version 12.6
User Manual
3/31/2025

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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

1. Dr.Web Security Space (macOS) 6
1.1. Conventions 6
1.2. About Dr.Web 6
1.3. System Requirements 7
2. Installing and Uninstalling 9
3. Full Disk Access 15
4. Managing Licenses 17
4.1. Trial Version 17
4.2. Purchasing License 17
4.3. License Activation 18
4.4. License Renewal 19
4.5. License Restoration 20
4.6. Serial Number 21
4.7. Key File 22
5. Dashboard 24
6. Notifications 26
7. Updating Virus Databases 28
8. Real-Time File System Protection 30
8.1. Configuring SpIDer Guard File Monitor 31
8.2. Excluding Files and Directories From Scanning 34
9. Web Traffic Scan 36
9.1. Configuring SpIDer Gate Internet Monitor 37
9.2. Excluding Websites From Scanning 41
9.3. Encrypted Traffic Scan 41
9.4. Excluding Applications From Scanning 42
10. Protection From Network Threats 44
10.1. Firewall Preferences 45
11. Scanning Mac on Demand 49
11.1. Scanner Preferences 52
11.2. Excluding Files and Directories From Scanning 55
12. Privacy Protection 57
12.1. Allowing Access to Camera and Microphone 57

13. Neutralizing Threats 59
13.1. Threats 59
13.2. Quarantine 60
14. Support 62
14.1. Help 62
14.2. Questions and Answers 62
14.3. Error Codes 68
14.4. Technical Support 74
15. General Preferences 75
16. Connection to Cloud Services 79
17. Centralized Protection Mode 80
18. Reference Information 86
18.1. Centralized Security Management and Anti-Virus Network 86
18.2. Threat Types 88
18.3. Detection Methods 92
18.4. Keyboard Shortcuts 94

1. Dr.Web Security Space (macOS)

1.1. Conventions

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

Convention	Comment
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`/Volumes/Macintosh HD/`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

1.2. About Dr.Web

Dr.Web protects Mac from various 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 (only for macOS 10.13 or earlier).

About the application

To open the application details window, click in the top left corner of the main window.

The information is specified in the following five tabs:

- **About Dr.Web**—application version, scan engine version, last update date, station ID, the option of generating a report for the support team (if enabled in the General section).
- **Help**—help describing Dr.Web operation.
- **News**—latest news on the Doctor Web website.
- **Promotions**—Doctor Web promotional offers.
- **About Viruses**—news about viruses found by Doctor Web virus analysts.

1.3. System Requirements

Parameter	Requirements
Device	Mac running macOS operating system. We cannot guarantee that Dr.Web will function correctly on non-Apple-branded computers
Free disk space	2 GB
Operating system	• OS X 10.11 El Capitan • macOS 10.12 Sierra • macOS 10.13 High Sierra • macOS 10.14 Mojave • macOS 10.15 Catalina • macOS 11 Big Sur • macOS 12 Monterey • macOS 13 Ventura • macOS 14 Sonoma • macOS 15 Sequoia We cannot guarantee that Dr.Web will function correctly on modified macOS systems or Hackintoshes

To ensure correct operation of Dr.Web, the following ports must be opened:

Purpose	Direction	Port numbers
To activate and renew the license	outgoing	443
To update	outgoing	80
To connect to Dr.Web Cloud	outgoing	UDP:

Purpose	Direction	Port numbers
		• 2075 TCP: • 3010, • 3020, • 3030, • 3040

How to check the version of Mac operating system

1. Go to Apple menu .
2. Click **About This Mac**.
3. (Only for macOS 12 and earlier versions) Select the **Overview** tab.

How to check the disk space on your Mac

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **About This Mac**.
3. Click **Storage** tab. You'll see an overview of your free space.

Click **Manage** to see the recommendations for optimizing your storage.

For macOS 13.0 and later versions

1. Go to Apple menu > **System Preferences**.
2. On the left, select **General**.
3. On the right, click **Storage**. You'll see an overview of your free space.

Additionally, in the **Recommendations** section, you can find suggestions about your storage optimization.

2. Installing and Uninstalling

Installing Dr.Web

To install Dr.Web

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 account password and click **Install Helper**.
6. If **System Extension Blocked** message appears, enable system extensions.
7. Dr.Web will be copied into the **Applications** folder and start automatically.
8. Enable Full Disk Access for Dr.Web.

To enable system extensions

For macOS 12.0 and earlier versions

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

> For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.

6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.
4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

To Enable Full Disk Access

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. If preferences are unavailable, unlock them. To do that, click at the bottom and enter your user name and password.
4. Click **Security & Privacy**.
5. Click **Privacy**.
6. Click **Full Disk Access**.
7. Add Dr.Web components to the list of allowed ones.
8. Click **Restart** for the changes to take effect.

For macOS 13.0 and later versions

1. In the main Dr.Web window, select .
2. In the **Preferences** window, select the **General** section.
3. Click **Allow access**.
4. In the Wizard that opens, click **Open System Settings**.
5. Click through the instructions in the Wizard until you see a Dr.Web icon.
6. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
7. To confirm, enter your user name and password in the pop-up.
8. Click **Quit & Reopen** for the changes to take effect.

If the **Allow access** button is greyed out, it means that full disk access is already allowed.

After the installation, the Dr.Web icon appears in the top macOS ribbon. It opens the Dr.Web.

When opened for the first time, Dr.Web updates the virus databases to the current state. After that, Dr.Web updates virus databases every 30 minutes. You can change the frequency of updates.

Installation errors

Unsupported Operating System

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

How to check the version of Mac operating system

1. Go to Apple menu .
2. Click **About This Mac**.
3. (Only for macOS 12 and earlier versions) Select the **Overview** tab.

Not Enough Disk Space

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

How to check the disk space on your Mac

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **About This Mac**.
3. Click **Storage** tab. You'll see an overview of your free space.

Click **Manage** to see the recommendations for optimizing your storage.

For macOS 13.0 and later versions

1. Go to Apple menu > **System Preferences**.
2. On the left, select **General**.
3. On the right, click **Storage**. You'll see an overview of your free space.

Additionally, in the **Recommendations** section, you can find suggestions about your storage optimization.

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 applications on one computer may lead to a system crash and loss of important data. This is why you should uninstall the previous Dr.Web version or other anti-virus installed on your Mac.

See how to uninstall third-party anti-virus software 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

Uninstalling Dr.Web

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

During uninstallation of Dr.Web, the key and configuration files, as well as the application preferences file are not removed from your Mac.

Do not use third-party applications to uninstall Dr.Web. It may lead to incomplete uninstallation of the application.

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

To uninstall Dr.Web manually

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

```
sudo /usr/bin/killall 'Dr.Web'

sudo /usr/bin/killall 'Dr.Web for macOS'

sudo /bin/launchctl bootout gui/$(id -u)/com.drweb.LoginLauncher

sudo /bin/launchctl remove com.drweb.pro.configd

sudo /bin/launchctl remove com.drweb.agent

sudo /bin/launchctl remove com.drweb.LoginLauncher

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'

sudo /sbin/kextunload -m com.drweb.kext.DrWebNetMonitor

sudo /sbin/kextunload -m com.drweb.kext.DrWebMonitor

sudo "/Applications/Dr.Web/Dr.Web for
macOS.app/Contents/Resources/Extensions/Dr.Web
Firewall.app/Contents/MacOS/Dr.Web Firewall" --deactivate

sudo "/Applications/Dr.Web/Dr.Web for
macOS.app/Contents/Resources/Extensions/Dr.Web
Spider.app/Contents/MacOS/Dr.Web Spider" --deactivate

sudo "/Applications/Dr.Web/Dr.Web.app/Contents/MacOS/Dr.Web\
Firewall.app/Contents/MacOS/Dr.Web\ Firewall" --deactivate

sudo "/Applications/Dr.Web/Dr.Web.app/Contents/MacOS/Dr.Web\
Spider.app/Contents/MacOS/Dr.Web\ Spider" --deactivate

sudo rm -Rf /usr/local/bin/drweb-ctl

sudo rm -Rf "/Library/LaunchDaemons/com.drweb.pro.configd.plist"

sudo rm -Rf "/Library/LaunchAgents/com.drweb.LoginLauncher.plist"

sudo rm -Rf "/Library/Application Support/DrWeb/mail"
```

```
sudo rm -Rf "/Library/Application Support/DrWeb/html"
sudo rm -Rf "/Library/Application Support/DrWeb/dws"
sudo rm -Rf "/Library/Application Support/DrWeb/var"
sudo rm -Rf "/Library/Application Support/DrWeb/bases"
sudo rm -Rf "/Library/Application Support/DrWeb/lib"
sudo rm -Rf "/Library/Application Support/DrWeb/bin"
sudo rm -Rf "/Library/Application Support/DrWeb/version"
sudo rm -Rf "/Library/Application Support/DrWeb/var"
sudo rm -Rf "/Library/Application Support/DrWeb/www"
sudo rm -Rf "/Library/Application Support/DrWeb/cache"
sudo rm -Rf "/Library/Application Support/DrWeb/update"
sudo rm -Rf "/Library/Application Support/DrWeb/install.plist"
sudo chflags -hv nouchg /Applications/Dr.Web
sudo chflags -hv nouchg "/Applications/Dr.Web/Dr.Web for macOS.app"
sudo chflags -hv nouchg "/Applications/Dr.Web/Uninstall Dr.Web.app"
sudo chflags -hv nouchg "/Applications/Dr.Web/Dr.Web.app"
sudo rm -Rf "/Applications/Dr.Web/Dr.Web for macOS.app"
sudo rm -Rf "/Applications/Dr.Web/Uninstall Dr.Web.app"
sudo rm -Rf "/Applications/Dr.Web/Dr.Web.app"
sudo rm -Rf /Applications/Dr.Web
```

3. Full Disk Access

To make sure that Dr.Web components operate correctly and protect your Mac, you need to allow *Full Disk Access* for the application.

You can do it

- From notifications on full disk access being required
- In Dr.Web preferences, the **General** section.

> Updating your Mac to macOS 13 Ventura will require you to grant Dr.Web full disk access again.

If you do not allow the access, the application will be displaying a notification that full disk access is required after each restart of your Mac.

Enabling Full Disk Access

In preferences

1. In the main window, click .
2. In the **Preferences** window, select the **General** section.
3. Click **Allow access**.
4. In the Wizard that opens, click **Open System Settings**.
5. Click through the instructions in the Wizard until you see a Dr.Web icon.
6. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
7. To confirm, enter your user name and password in the pop-up.
8. Click **Quit & Reopen** for the changes to take effect.

> If the **Allow access** button is greyed out, it means that full disk access is already allowed.

From notifications

1. Click **Allow access**.
2. In the Wizard that opens, click **Open System Settings**.
3. Click through the instructions in the Wizard until you see a Dr.Web icon.

4. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
5. To confirm, enter your user name and password in the pop-up.
6. Click **Quit & Reopen** for the changes to take effect.

To enable full disk access through system settings of your Mac without the Wizard, you need to drag and drop all Dr.Web components to the settings window. To avoid mistakes, we recommend that you use the Wizard instead.

4. Managing Licenses

A license is required to use Dr.Web. You can purchase it on the Doctor Web website or through authorized partners. The license allows you to use all application features during the entire license period. User rights are set in accordance with the License Agreement, which users are required to accept during 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 features before purchasing it, you can activate a trial version. All features and protection components of the application are available in the trial version.

4.1. Trial Version

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

You can only activate a trial version on the same computer once a year.

You can activate a trial version:

- For 1 month. You don't need to register or specify a serial number. The license is activated automatically.

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**.

4.2. 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 and an attached key file.

4.3. License Activation

To get access to all functions and components of the application, activate your license. We recommend that you activate your license right after installing the application. It is required for virus databases to update and application components to operate, 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 application window. You can activate your license using a key file, a serial number, or a configuration file (.cfg).

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**.

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 into the dotted rectangular box 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**.

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 when the application is already running.
- 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 when the application is already running.

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 that you own this license.

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.

4.4. License Renewal

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

How to 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 to 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 on-the-fly updates, so you do not need to reinstall the application 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 into the dotted rectangular box or click to choose the file on your Mac.

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

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

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

4.5. License Restoration

If the key file is lost or corrupted, the operation of all Dr.Web components will be blocked and the security of your Mac 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 as follows:

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

You can reactivate the license if it has not expired.

A license key file can be obtained through the application a limited number of times. If that amount has been exceeded, you can confirm the registration of your serial number at https://products.drweb.com/register/ to receive the key file. The key file is sent to the email that was specified during the first registration.

4.6. Serial Number

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

Where to 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, your serial number will be stored on the Allsoft.ru website in the Personal section under order details.
  - 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 the My purchases service.
- If you purchased your license in a box, you can find your serial number in the License certificate.
- If you purchased your license from a retailer, you can find your serial number on the receipt.

If your serial number is registered

- If Dr.Web is installed on your device, download this file and unpack it. Double-click 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 serial 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 the 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 as follows:

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

4.7. 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 where Dr.Web can operate).

The key file is located in the Dr.Web installation folder. The application 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 these conditions is violated, the key file gets *invalid*, and Dr.Web stops detecting and neutralizing malicious software.

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.

5. 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 (only for macOS 10.13 or earlier),
- 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 applications 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 virus detection component with the following features:

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

Privacy Protection

- **Camera**—camera access control for applications.
- **Microphone**—microphone access control for applications.

Camera and microphone access control settings are not available on macOS 10.14 and later versions.

Update

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

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. Alternatively, you can purchase 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 where infected files and other threats are isolated, so that they cannot threaten the system.

6. Notifications

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

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

> Notifications of attempts to connect to your microphone or camera are available on macOS 10.13 or earlier versions.

Dr.Web uses macOS system notifications to display messages on detected and neutralized threats or errors in the operation of components. You can disable or configure system notifications from Dr.Web.

To disable system notifications

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. Click **Notifications** (for macOS 12.0, **Notifications & Focus** > **Notifications**).
4. Select Dr.Web for macOS on the left-hand side, then turn off **Allow notifications** on the right.

> There is no toggle in macOS 10.14 and earlier versions. To disable notifications, clear all check boxes.

For macOS 13.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Notifications** in the sidebar.
4. Below **Application Notifications** on the right, click Dr.Web for macOS and turn off **Allow**

notifications.

To configure system notifications

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. Click **Notifications** (for macOS 12.0, **Notifications & Focus** > **Notifications**).
4. Select Dr.Web for macOS on the left-hand side, then customize the style and other settings for notifications on the right.

For macOS 13.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Notifications** in the sidebar.
4. Below **Application Notifications** on the right, click Dr.Web for macOS, then customize the style and other settings for notifications.

7. Updating Virus Databases

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

New types of threats with more advanced disguise features appear every day. Updating Dr.Web allows to detect previously unknown viruses, to block their spreading and sometimes to cure infected files that were incurable before. Make sure to update virus databases in a timely manner, as they will become outdated after 24 hours since the last successful update.

Internet connection is required to update virus databases.

When opened for the first time, Dr.Web updates the virus databases to the current state. After that, Dr.Web updates virus databases every 30 minutes. You can change the frequency of updates.

To change the frequency of virus database updates

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. Choose an update frequency from the **Update Virus Databases** drop-down list.

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

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 the address and port for the proxy server.
7. If the proxy server requires a password, select the **Protect proxy server with a password** check box.
8. Specify your user name and password.
9. Click **Save**.

8. Real-Time File System Protection

The SpIDer Guard file system monitor scans all files that users open in real time and monitors all applications 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 system startup and works constantly in the background.

When SpIDer Guard detects threats, it displays a warning and applies an 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 rights 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 resume 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. When it happens, SpIDer Guard doesn’t work, and you see a notification saying that the system extension was blocked. For the real-time file system scan to operate correctly, allow the loading of system software from Doctor Web Ltd.

To enable system extensions

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. Click **Security & Privacy**.

4. If preferences are unavailable, unlock them. To do that, click  at the bottom and enter your user name and password.
5. Click **Allow** next to the message about blocking Doctor Web Ltd.'s system software.

For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.
6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.
4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

8.1. 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, which are objects infected with known and potentially curable viruses. Suspicious objects and various types of malware 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 curing attempt 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 Trojans 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 Trojans 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.

Actions applied to threats detected by SpIDer Guard

Object type	Action				
	Cure, move to quarantine if incurable	Cure, delete if incurable	Move to quarantine	Delete	Ignore
Infected	+/*	+	+	+	
Suspicious			+/*	+	+
Adware			+/*	+	+
Dialers			+/*	+	+
Jokes			+	+	+/*

Object type	Action				
	Cure, move to quarantine if incurable	Cure, delete if incurable	Move to quarantine	Delete	Ignore
Riskware			+	+	+/*
Hacktools			+	+	+/*
Infected archives	+	+	+	+	+
Infected email files	+	+	+	+	+

Conventions

+	available action
+/*	action set by default

Infected archives and email files do not have a default action assigned to them, as the action depends on the type of threat detected. If multiple threats are identified, then the action will be based on the most significant of them.

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 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 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 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**.

8.2. 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 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 application window.
- To clear the exclusion list, select all the objects in the list (COMMAND-A) and click  .

Default exclusion preferences are optimal for most uses. Do not make any unnecessary changes.

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.

9. 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 system startup 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 certain websites and website categories.

You can also exclude certain 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 enable system extensions

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.

3. Click **Security & Privacy**.
4. If preferences are unavailable, unlock them. To do that, click  at the bottom and enter your user name and password.
5. Click **Allow** next to the message about blocking Doctor Web Ltd.'s system software.

For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.
6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.
4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

9.1. 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 software, 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 change default preferences for no reason.

Threat scanning

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

SpIDer Gate restricts access to non-recommended websites and addresses 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**.

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 objects** check box.

By default, SpIDer Gate blocks suspicious software, adware and dialers. You can configure blocking of malware types.

To configure blocking of malware

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 a time limit 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.

URL filter

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 and so on.

Category	Description
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 betting websites and so on.
Drugs	Websites that promote use, production or distribution of drugs and so on.
Online games	Websites that provide access to games using the permanent internet connection.
Terrorism	Websites that contain violent and propaganda materials or terrorist attack descriptions and so on.
Obscene language	Websites that contain obscene language (in titles, articles and so on).
Chats	Websites that offer a real-time transmission of text messages.
Email	Websites that offer free registration of an email box.
Social networks	Various social networking services: general, professional, corporate, interest-based; themed dating websites.
Anonimizers	Websites that allow users to hide personal information and gain access to restricted web resources.
Cryptocurrency mining pools	Websites that provide access to common services for cryptocurrency mining.
Jobs	Job search 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.

9.2. 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 exclusions list, select it and click or drag it outside the application window.
- To clear the exclusion list, select all objects in the list (COMMAND-A) and click .

9.3. 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 is a security certificate?

A security certificate is an electronic document that confirms that the certified application has been tested in a certification center.

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

When you install Dr.Web, 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 such applications, you can export Doctor Web certificate manually and then install (import) it in the target 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 importing certificates in the user documentation of the target application.

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 scanning.

9.4. Excluding Applications From Scanning

You can exclude network connections of certain applications from scanning. Such applications will connect freely regardless of SpIDer Gate internet monitor preferences.

To exclude network connections of applications from scanning

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 exclusions list, select it and click or drag it outside the application window.
- To clear the exclusion list, select all objects in the list (COMMAND-A) and click  .

10. 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 system startup and operates 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

If Firewall is enabled, third-party applications for scanning web traffic and controlling access to web resources installed on your Mac may not work properly.

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 enable system extensions

For macOS 12.0 and earlier versions

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

For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.
6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.
4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

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.

10.1. 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 the 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. 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.

All connections are allowed by default.

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 **Mode** drop-down list.

Filtering rules

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

A filtering rule includes:

- Application file in the `.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 **Add application** 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, the rule will apply to all 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 the IP address or the 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 will open.

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

5. Edit the parameters for the rule.
6. Click **Save**.

11. Scanning Mac on Demand

Dr.Web Scanner scans objects in the file system on demand and detects various threats that can hide in the system. To protect your computer, we recommend that you regularly 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, scanning is paused to prevent the battery from draining fast. Dr.Web displays a notification and lets you decide whether to continue scanning or not. When you use a charge cable to power your Mac, 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 rights) ⚠ 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

You can scan specific files or folders using any of the following methods.

From the Scan Your Mac section

1. On the **Dashboard** tab of the main window, choose **Scan Your Mac**.
2. Drag files and folders that you want to scan into the dotted rectangular box or click this box to choose the file or folder.

By dragging onto the app icon

1. Drag files and folders that you want to check onto the app icon in the menu bar (this runs along the top of the screen on your Mac).

From the context 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 permissions to apply action to the object.	Start scanning with administrative rights.
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 the file 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 rights

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

To start scanning with administrative rights

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.

11.1. 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 applications 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 curing attempt 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 Trojans 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 Trojans 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 password to change the Scanner preferences. Preferences are automatically changed for all Mac users.

Do not unnecessarily change default preferences of automatic actions.

Actions applied to threats detected by Scanner

Object type	Action				
	Cure, move to quarantine if incurable	Cure, delete if incurable	Move to quarantine	Delete	Ignore
Infected	+/*	+	+	+	
Suspicious			+/*	+	+
Adware			+/*	+	+
Dialers			+/*	+	+
Jokes			+	+	+/*
Riskware			+	+	+/*
Hacktools			+	+	+/*
Infected archives	+	+	+	+	+
Infected email files	+	+	+	+	+

Conventions

+	available action
+/*	action set by default

Infected archives and email files do not have a default action assigned to them, as the action depends on the type of threat detected. If multiple threats are identified, then the action will be based on the most significant of them.

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 rights

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

To start scanning with administrative rights

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 password before each scan.

You can also configure scanning on demand: enable scanning of archives and emails, or specify the time limit 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, scanning is paused to prevent the battery from draining fast. Dr.Web displays a notification and lets you decide whether to continue scanning or not. When you use a charge cable to power your Mac, 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.
5. Click **Save**.

11.2. 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 password.
5. Click the button and select a folder or file that you want to exclude, or simply drag it to the exclusion 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 exclusions list, clear the **Scanner** check box next to the object.

- To remove an object from the exclusions list, select it and click or drag it outside the application window.

- To clear the exclusion list, select all the objects in the list (COMMAND-A) and click −.

Default exclusions preferences are optimal for most uses. Do not make any unnecessary changes.

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.

12. Privacy Protection

Dr.Web protects your privacy by controlling access of applications 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 settings are not available on macOS 10.14 and later versions.

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 access your camera or microphone, Dr.Web will display a notification and ask what action should be applied.

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

  Users from the Administrators group have more access control options.
  - **Allow once**—allows the application to access your camera or microphone once.
  - **Always allow**—allows the application to permanently access your camera or microphone.

  If you choose the **Always allow** option, Dr.Web will create a rule for this application in the exclusions list.

> To create a rule in the exclusions list, you need administrator rights.

12.1. Allowing 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 versions.

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 password.
5. Click  under the **Camera** or **Microphone** lists, select the application you need and drag it to the corresponding list.

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

13. Neutralizing Threats

13.1. 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 an 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 an 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 application preferences for the corresponding types of threats.

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

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

To apply the action to several threats

1. Select several threats using the SHIFT key.

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

13.2. 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 privacy reasons, the quarantine folder is created for each user in the system. If you switch to administrator mode, the detected threats moved to the administrator quarantine 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 update of the application.

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

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

To apply the action to several threats

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

14. Support

14.1. 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 have not been able to find the answer, contact Doctor Web technical support.

14.2. 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

How to change a language

You can only change a language on macOS 10.15 or later versions.

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Language & Region**.
4. Click **Applications**.
5. Choose **Dr.Web**, then pick the application language you need.

For macOS 13.0 and later versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. Click **General**.
4. Click **Language & Region**.

5. Click **Applications**.
6. Choose **Dr.Web**, then pick the application language you need.

SpIDer Gate, SpIDer Guard, and Firewall are disabled

macOS blocks kernel (system) extension loading. For SpIDer Gate and SpIDer Guard to operate correctly, allow loading of Doctor Web Ltd.'s system software as described below.

To enable system extensions

For macOS 12.0 and earlier versions

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

> For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.
6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.

4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

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

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

Dr.Web freezes 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 the macOS standard tool Activity monitor.

If the issue persists, try reinstalling the application.

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.

VPN tunnel in AdGuard doesn't work

If AdGuard VPN tunnel works incorrectly, do the following steps:

1. Open AdGuard preferences.
2. Click **Network**.
3. Make sure that the **Automatically filter applications** check box is selected.
4. Click **Applications**.
5. Add Dr.Web for macOS to the list of filtered applications.

If you can't find Dr.Web for macOS to add to the list of filtered applications, reset your Mac and try again.

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 your license period, go to the **License** section of Dr.Web main window. If the license expired, buy the new one.

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.
- Freezes 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 the 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 rights to access such files. If there are archives in the list of skipped objects, try to unpack them before scanning.

Scanner freezes

If Scanner freezes, close and restart the application. If the issue persists, reinstall the application.

Read error

This issue can occur if you didn't enable full disk access for Dr.Web.

To Enable Full Disk Access

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. If preferences are unavailable, unlock them. To do that, click at the bottom and enter your user name and password.
4. Click **Security & Privacy**.
5. Click **Privacy**.
6. Click **Full Disk Access**.
7. Add Dr.Web components to the list of allowed ones.
8. Click **Restart** for the changes to take effect.

For macOS 13.0 and later versions

1. In the main Dr.Web window, select .
2. In the **Preferences** window, select the **General** section.
3. Click **Allow access**.
4. In the Wizard that opens, click **Open System Settings**.
5. Click through the instructions in the Wizard until you see a Dr.Web icon.
6. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
7. To confirm, enter your user name and password in the pop-up.
8. Click **Quit & Reopen** for the changes to take effect.

If the **Allow access** button is greyed out, it means that full disk access is already allowed.

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, then restart the browser.
- Check if the website uses a secure connection (if it does, a lock appears in the browser address bar). If a secure connection is used, select the **Scan encrypted traffic** check box on the Network tab and restart the browser.
- SpIDer Gate does not block websites that connect through FTP/SPDY or HTTP/2.0.

Certificate error message appears when opening the website

- This 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 the browser or mail client was opened immediately after the installation, it might not have obtained the system security certificate. In this case, 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 the error persists, then the certificate is untrusted and we do not recommend that you 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, turn it off and run an update again. To run the update manually, select **Update Is Required** in Dr.Web menu .
- If the router is working in the Connection on demand mode, make sure that the connection is constantly active (maximum idle time is 0).

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

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 the 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 a new trial version using another email address.

Unable to activate the license

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

If you have issues with the operation of Dr.Web that are not described above, contact Doctor Web technical support. Make sure that you give Doctor Web specialists as much information as possible about the problem, so that they help you as quickly as possible.

14.3. 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 a pending state (probably, network connection is currently being establishing or one of the application components is loading or initializing, which takes a long time).

Code	Error	Description
4	Interrupted by user	Action is terminated by the user (probably, the action was taking too much time).
5	Operation canceled	Action is cancelled (probably, the action was taking too much time).
6	IPC connection terminated	Inter-process communication (IPC) connection with one of the components is terminated (most likely, the component shuts down because of the user command or being idle).
7	Invalid IPC message size	Message of an invalid size is received during the component inter-process communication (IPC).
8	Invalid IPC message format	Message of an invalid format is received during the component inter-process communication (IPC).
9	Not ready	Required action cannot be performed because the required component or device is not initialized yet.
10	Component is not installed	Some function of Dr.Web 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 was probably removed.
24	Access denied	Insufficient rights to access the 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.

Code	Error	Description
26	Data file corrupted	Requested data is corrupted.
27	File already exists	When attempting to create a file, another file with the same name is detected.
28	Read-only file system	When attempting 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 failed).
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 the file scan, 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, a directory, socket, or other object of the file system).
34	Name already in use	When attempting 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	An attempt to restore a file requires to move it between file system directories belonging to different mount points.
38	Unpacking error	Archive unpacking failed (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 an earlier application 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	Current virus database combination is not supported.

Code	Error	Description
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 the required permissions.
49	Access token is invalid	One of the application components provides an invalid authorization token when attempting to access the operation that required elevated permissions.
60	Invalid argument	An invalid argument is used when attempting to run a command.
61	Invalid operation	An attempt to run an invalid command is detected.
62	Root access required	Only a user with root access can perform this action.
63	Not allowed in the centralized protection mode	The required action can be performed only if the application operates in the standalone mode.
64	Non-supported OS	The application does not support the 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 application.
66	Unknown option	The configuration file contains parameters unknown or not supported in the current version of the application.
67	Unknown section	The configuration file contains sections unknown or not supported in the current version of the application.
68	Invalid option value	One of the parameters in the configuration file contains an invalid value.
69	Invalid state	The application 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 instead of a single value.
71	Tag value is invalid	Invalid tag detected in one of the sections in the configuration file with a name containing a unique tag identifier.
80	Record not found	The accessed threat record is missing (probably, another application component processed the threat).

Code	Error	Description
81	Record is in process now	The accessed threat record is being processed by another application component.
82	File has already been quarantined	When attempting to move the file with the detected threat to quarantine, it was detected that the file is already in quarantine (most likely, another application component processed the threat).
89	Cannot backup before update	An attempt to make a backup copy of the files before downloading updates from the update server 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	Application fails to connect to update servers using the proxy server specified in preferences.
94	No update servers available	Application 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 the downloaded file containing updates is invalid.
99	Invalid demo key file	Current demo key file is invalid (for example, it was received from another computer).
100	License key file is blocked	Current license is blocked (probably, the license agreement conditions on using Dr.Web were violated).
101	Invalid license	Current license is meant for another product or does not allow operation of the installed product components.
102	Invalid configuration	One of the application components cannot be in operation because of incorrect configuration preferences.
104	Invalid executable file	One of the application 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 required for threat detection is missing or unavailable.

Code	Error	Description
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	An application component cannot be in operation because incompatible software is detected. This software interrupts correct component operation.
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 the Scanner component used for this feature is missing.
121	ESAgent is not available	The ESAgent component is missing. This component is necessary to connect to the centralized protection server.
122	Firewall is not available	Cannot control network connections as the Firewall component is missing or failed to start. This module is used to redirect connections.
123	Network Checker is not available	Cannot control network connections as the 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.

14.4. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

1. Download and review the latest manuals and guides at https://download.drweb.com/doc/.
2. See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
3. Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

1. Fill out a web form in the appropriate section at https://support.drweb.com/.
2. Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.

15. General Preferences

In the **General** section, you can configure sound alerts, on-screen notifications, restore default preferences, and set up event logging for technical support.

You do not have to enter your user name and the password to change general preferences. Preferences are automatically changed for all Mac users.

This menu allows you to configure notifications only if you run macOS 10.14 or earlier versions. In later Mac versions, configure notifications in the **System Preferences** menu of your Mac.

Notifications

Dr.Web uses macOS system notifications to display messages on detected and neutralized threats or errors in the operation of components.

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 detected, neutralized, and removed threats.

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 application 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 password.
4. Click **Restore Defaults**.
5. Click **Restore** to confirm restoring default application preferences.

Configuring event logging

Enable event logging to be able to generate reports for technical support.

To enable event logging

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 password.
4. Check the **Enable logging** check box.

You can also configure how Dr.Web events will be classified in the logs, thus configuring which information will show in your report for the technical support team.

To configure the classification for Dr.Web module event log

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 password.
4. Check the **Enable logging** check box.
5. Click **Configure**.
6. Select the required classification for each module.
7. Click **Save**.

You can configure event classification for the following modules and products:

- ConfigD
- SpIDer Guard
- ScanningEngine

- FileCheck
- Firewall
- GateD
- NetCheck
- UrlCheck
- Dr.Web for MacOS
- Updater
- Dr.Web Agent

In the table below, see available event classifications and their descriptions.

Classification	Description
DEBUG	The most detailed event description for debugging. The report will contain all messages that may help troubleshoot.
INFO	The report will contain all messages, including those about normal system operation, start of scheduled tasks, start and shutdown of services, processes, and user actions.
NOTICE	The report will contain all error messages, notifications, and warnings.
WARNING	The report will contain all error messages and warnings.
ERROR	The report will contain only error messages.

Full Disk Access

To Enable Full Disk Access

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. If preferences are unavailable, unlock them. To do that, click at the bottom and enter your user name and password.
4. Click **Security & Privacy**.
5. Click **Privacy**.
6. Click **Full Disk Access**.
7. Add Dr.Web components to the list of allowed ones.
8. Click **Restart** for the changes to take effect.

For macOS 13.0 and later versions

1. In the main Dr.Web window, select  .
2. In the **Preferences** window, select the **General** section.
3. Click **Allow access**.
4. In the Wizard that opens, click **Open System Settings**.
5. Click through the instructions in the Wizard until you see a Dr.Web icon.
6. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
7. To confirm, enter your user name and password in the pop-up.
8. Click **Quit & Reopen** for the changes to take effect.

If the **Allow access** button is greyed out, it means that full disk access is already allowed.

16. Connection to Cloud Services

Dr.Web connects to Doctor Web cloud services to protect your Mac from the latest threats and improve the operation of application 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. Cloud services process the data faster than local virus databases are updated on the computer.

Dr.Web automatically sends anonymized data about component operation to Doctor Web servers. You can read the privacy policy statement on the 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.

17. Centralized Protection Mode

Centralized protection of your Mac is provided by Dr.Web Enterprise Security Suite server administrator or by your IT service provider through the Dr.Web AV-Desk anti-virus service. Your personal license is not required for operation in the centralized 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 services purchased from your provider. The following preferences and components can be controlled from the server:

- Virus database updates. Updates are downloaded automatically from the centralized protection server. If the server is unavailable, updates are downloaded from Dr.Web internet 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 on schedule.

Connecting Mac

Every Mac with an installed Dr.Web is an individual station. Depending on the authorization preferences of the centralized protection server, the 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, where Dr.Web creates a new ID and a password. In this case, the station may require server authorization or be authorized automatically, 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 Administrator Manual** and the **Dr.Web AV-Desk Administrator Manual**.

Automatic connection

If you've purchased subscription to the Dr.Web AV-Desk anti-virus service, you can install Dr.Web using a `.run` file with server connection parameters. Contact your IT provider to obtain the `.run` file.

To install Dr.Web using the .run file

1. Make the `.run` file executable.
2. Run the `.run` file.
3. Click **Install Dr.Web**.
4. Accept the terms of the License Agreement. The installation process will start.
5. Enter the administrator password and click **Install Helper**.
6. If **System Extension Blocked** message appears, enable system extensions.
7. Dr.Web will be copied into the **Applications** folder and start automatically.
8. Enable Full Disk Access for Dr.Web.

To make the .run file executable

1. Open **Terminal**.
2. Go to the directory that contains your .run file:

```
cd <your-directory>
```

3. Run the following command:

```
chmod 0755 <your-file-name>.run
```

Example:

```
cd Desktop
chmod 0755 drweb-12.5.0-av-macosx.run
```

To enable system extensions

For macOS 12.0 and earlier versions

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

For macOS 11.0 and 12.0, click **Advanced** and select Dr.Web components.

For macOS 13.0 and 14.0

1. Go to Apple menu .
2. Click **System Settings**.
3. Click **Privacy & Security**.
4. In this section, scroll down to the phrase **Some system software requires your attention before it can be used** and click **Details**.
5. To unlock settings, enter your user name and password in the pop-up.
6. Turn on the toggles next to Dr.Web components and click **OK**.

For macOS 15.0 and later versions

1. Go to Apple menu .
2. Click **System Settings**.
3. Go to **General** and select **Login Items & Extensions**.
4. In the **Extensions** subsection scroll down to **Endpoint Security Extensions** and click ⓘ next to it.
5. Turn on the **Dr.Web Spider** toggle and click **OK**.
6. In the **Extensions** subsection scroll down to **Network Extensions** and click ⓘ next to it.
7. Turn on the **Dr.Web Firewall** toggle and click **Done**.

To Enable Full Disk Access

For macOS 12.0 and earlier versions

1. Go to Apple menu .
2. Click **System Preferences**.
3. If preferences are unavailable, unlock them. To do that, click at the bottom and enter your user name and password.
4. Click **Security & Privacy**.
5. Click **Privacy**.
6. Click **Full Disk Access**.
7. Add Dr.Web components to the list of allowed ones.
8. Click **Restart** for the changes to take effect.

For macOS 13.0 and later versions

1. In the main Dr.Web window, select .

2. In the **Preferences** window, select the **General** section.
3. Click **Allow access**.
4. In the Wizard that opens, click **Open System Settings**.
5. Click through the instructions in the Wizard until you see a Dr.Web icon.
6. Drag and drop the Dr.Web icon from the Wizard to the system settings section, which the Wizard refers to.
7. To confirm, enter your user name and password in the pop-up.
8. Click **Quit & Reopen** for the changes to take effect.

If the **Allow access** button is greyed out, it means that full disk access is already allowed.

If you received the `install.cfg` configuration file from your anti-virus network administrator or IT service provider, you can connect Dr.Web in the **License Activation** section. Connection to the centralized protection server will be configured automatically.

To connect the station using a configuration 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 configuration file into the dotted rectangular box or click to choose the file on your Mac.
5. Once the activation is completed, server connection will be automatically configured.

If your anti-virus network administrator provided you with a certificate, 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. Select the **Enable centralized protection mode** check box. Once the centralized protection mode is enabled, parameters of the last connection are restored.
5. Specify server IP address and port number for connecting to the server.

6. Drag a certificate to the dotted rectangular box 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 authorization parameters for your workstation.
   - Station ID
   - Password (assigned to your computer for registration on the server)
   - Traffic compression mode
   - Traffic encryption mode

   Values you enter are saved using the Keychain system and you don't need to enter them again when reconnecting to the server.
9. Click **Connect**.

Connecting a new station

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

To connect a new station

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. Select the **Enable centralized protection mode** check box.
5. Specify server IP address and port number for connecting to the server.
6. Drag a certificate to the dotted rectangular box 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 centralized protection mode and restore standalone operation of Dr.Web.

When you switch to this mode, all application preferences are restored to their previous or default states and all Dr.Web components become available to you again.

For correct operation in the standalone mode, Dr.Web requires a valid personal license key file. License received from the centralized 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 centralized protection mode** check box.
5. Click **Disable** to confirm the action.

18. Reference Information

18.1. Centralized Security Management and Anti-Virus Network

Solutions for centralized security management by 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 added to a single *anti-virus network* and administrators monitor and manage their security from the centralized server. Connection to a centralized anti-virus system ensures high level of protection with minimum effort from end-users.

Logical structure of anti-virus networks

Doctor Web solutions for centralized security management use *the client-server model* (see the figure below).

Local anti-virus *components* (clients, such as Dr.Web) protect computers of the company or users of IT service provider. Anti-virus components ensure protection and help connect to the centralized protection server.

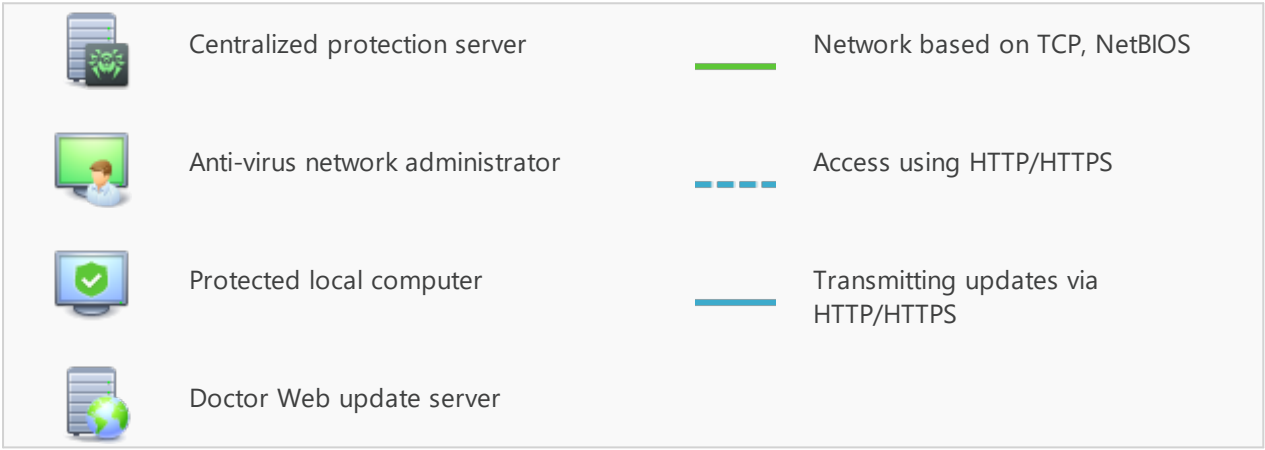

Figure 1. Logical structure of the anti-virus network

Local computers are updated and configured from the *centralized protection server*. The flow of instructions, data and statistics in the anti-virus network goes also through the centralized protection server. The amount of traffic between protected computers and the centralized server can be substantial, which is mitigated by traffic compression options. To prevent leaks of sensitive data or substitution of software downloaded onto protected computers, the solutions also support encryption.

Updates to the centralized protection server are delivered from Dr.Web update servers.

Local anti-virus components are configured and managed from the centralized protection server as required by *anti-virus network administrators*. Administrators manage centralized protection servers and the topology of anti-virus networks (for example, validate connections to centralized protection server from remote computers), as well as configure 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 centralized protection mode. Installing two anti-virus apps on one computer may lead to a system crash and loss of important data.

Centralized security solutions

Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite is a complex solution for corporate networks of any scale. It protects workstations, mail and file servers from all types of modern information security threats. It also contains diverse tools that help anti-virus network administrators track and manage local anti-virus components, for example, deploy and update software, monitor the network status, collect statistics, and receive notifications of malware events.

Dr.Web AV-Desk internet service

Dr.Web AV-Desk is Doctor Web's novel internet service for online service providers. With this solution, providers can deliver information security services to individual and corporate customers by offering them service packages that may include protection from viruses, spam and other computer threats for as long as necessary. Services are provided online.

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

18.2. 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 software types stated below have the ability to endanger user data or confidentiality. Applications 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 software. 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.

18.3. Detection Methods

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which helps them thoroughly check suspicious files and control software behavior.

Signature analysis

The scans start with a signature analysis, which consists of comparing file code segments with 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 the signatures, ensuring correct virus detection and neutralization. Dr.Web virus databases are compiled in such a way that some entries can be used to detect not just specific viruses, but entire classes of threats.

Origins Tracing

After the signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing method to detect new and modified viruses with known infection mechanisms. Thus, Dr.Web users are protected against such threats as the notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, Origins Tracing can considerably reduce false triggering of the heuristic analyzer. Names of objects detected by the Origins Tracing algorithm have `.Origin` added to them.

Execution emulation

Program code emulation is used for detection of polymorphic and encrypted viruses when a search by checksums cannot be performed directly, or is very difficult (due to inability to build a reliable signature). This method involves simulating the execution of an analyzed code by an *emulator*—a programming model of the processor and runtime environment. An emulator operates within a protected memory region *(an emulator buffer*), in which execution of the analyzed application 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 by using a heuristic analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) that might be typical for a virus code, or, on the contrary, extremely rare in viruses. Each attribute has a weight, which determines the level of its severity and reliability. The weight 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 total 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 applications. 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.

Like any other 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".

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 constant updates of the virus databases that are 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.

18.4. 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
General	COMMAND-A	Select all
	COMMAND-W	Close