

The Kaspersky logo, consisting of the word "kaspersky" in a lowercase, bold, sans-serif font. The background of the entire page is a teal-to-green gradient with a large white rounded rectangle in the center. The logo is positioned in the upper left area of the white rectangle.

kaspersky

Kaspersky VPN for Mac

© 2022 AO Kaspersky Lab

Contents

[Kaspersky VPN help](#)

[Kaspersky VPN overview](#)

[FAQ](#)

[Hardware and software requirements](#)

[Install and uninstall the application](#)

[Connect to My Kaspersky](#)

[Kaspersky VPN versions](#)

[Upgrade to the Unlimited version](#)

[Protect your connection to an unsecured Wi-Fi network](#)

[Why is it impossible to open a website with Kaspersky VPN enabled?](#)

[Subscription & account](#)

[Kaspersky VPN versions](#)

[Upgrade to the Unlimited version](#)

[Restore your subscription](#)

[Change the My Kaspersky account](#)

[About the subscription](#)

[About anonymous subscriptions](#)

[Data provision](#)

[About data provided](#)

[Compliance with European Union law](#)

[Contents of trace files, dump files, and settings files](#)

[Get started with the application](#)

[Hardware and software requirements](#)

[Install and uninstall the application](#)

[Start the application for the first time](#)

[Connect to My Kaspersky](#)

[About two-step verification](#)

[Perform common tasks](#)

[Activate VPN connection](#)

[Select a VPN server](#)

[View the amount of used and available traffic](#)

[How to configure Split Tunneling](#)

[Protect your data if your secure connection is lost](#)

[Set up VPN settings for known Wi-Fi networks](#)

[Enable or disable sending data for marketing purposes](#)

[Enable tracing](#)

[Protect your connection to an unsecured Wi-Fi network](#)

[Select the action Kaspersky VPN performs when you join an unsecured Wi-Fi network](#)

[How to get customer service](#)

[Known issues](#)

[Sources of information about the application](#)

[Legal](#)

[View the terms and conditions of the End User License Agreement and the Marketing Statement](#)

[Information about third-party code](#)

[Trademark notices](#)

Kaspersky VPN help

Welcome to Kaspersky VPN

- [Kaspersky VPN overview](#)

Getting started

- [Hardware and software requirements](#)
- [Install Kaspersky VPN](#)
- [Initial setup](#)

Perform common tasks

- [Activate VPN connection](#)
- [Select a VPN server](#)
- [Protect your data if your secure connection is lost](#)
- [Set up VPN settings for known Wi-Fi networks](#)
- [How to configure Split Tunneling](#)

Personal data protection

- [About data provided](#)
- [Compliance with European Union law](#)
- [Contents of trace files, dump files, and settings files](#)

Contact Customer Service

- [How to contact Customer Service](#)

Kaspersky VPN overview

Kaspersky VPN Secure Connection (hereinafter – Kaspersky VPN) hides your real location and encrypts all data sent and received by your Mac. You can install Kaspersky VPN on desktop computers, laptops, and mobile devices running Microsoft® Windows®, macOS, Android™, or iOS™. You can use Kaspersky VPN for different types of network connections, for example, Wi-Fi, local internet connections, or USB modem connections.

Note: You can find information about features and improvements of the current and previous versions of the application [on the App Store](#) ².

Don't give up your privacy on the internet

Public Wi-Fi networks may be under-protected, for example, if a Wi-Fi network uses a vulnerable encryption protocol. Kaspersky VPN establishes an encrypted secure connection with websites that you visit so that no hackers can intercept your encrypted data.

Choose the optimal route to websites that you visit

When you use Kaspersky VPN, you can [select a VPN server](#) and appear to the internet as a visitor from another country. You can also view content regardless of regional restrictions.

Let Kaspersky VPN automatically protect unsecured connections

You can set the application to [automatically turn on VPN when you join unsecured Wi-Fi networks](#).

Let Kaspersky VPN automatically protect your connection

You can set the application to [automatically turn on VPN when your Mac starts](#).

Protect your data if your secure connection is lost

You can [use Kill Switch](#) to set the application to automatically cut the internet connection entirely if your VPN connection drops.

FAQ

Hardware and software requirements

Kaspersky VPN has the following hardware and software requirements:

- 1 GB of memory (RAM)
- 320 MB of free disk space
- Operating system macOS 11-13
- Internet connection
- Processor type: Intel, Apple silicon

Install and uninstall the application

You can install Kaspersky VPN from the App Store.

To install the application:

1. Open the App Store application.
2. Find Kaspersky VPN and install the application.

The App Store may prompt you to enter your Apple ID credentials.

Note: For more information on using the App Store and installing applications, refer to the relevant user guides for your Mac.

To uninstall the application:

1. Locate the application in the Finder.
2. Open the shortcut menu and choose **Move to Trash**.

Note: For more information on uninstalling applications, refer to the relevant user guides for your Mac.

Connect to My Kaspersky

When you open Kaspersky VPN, you can sign in to [My Kaspersky](#) with a [My Kaspersky account](#). If you have used another Kaspersky application, for example, Kaspersky VPN for another device or Kaspersky Internet Security, you probably already have a My Kaspersky account. Use it to sign in. If you don't have an account, you can create one.

Note: If you have signed in to My Kaspersky in another Kaspersky application on your Mac, the Kaspersky VPN application prompts you to sign in to My Kaspersky using the same account after the application installation.

[Sign in to My Kaspersky using your existing account](#)

1. Open the main application window and click **Sign In**.

The **Sign In to My Kaspersky** window opens.

2. Do one of the following:

- If you want to connect to My Kaspersky with your Google, Facebook, or Apple account, click the corresponding button and follow the instructions. For more details, see the [My Kaspersky help](#) . If you don't have a My Kaspersky account yet, the application will prompt you to register on My Kaspersky.

Note: The availability of the option to sign in with Facebook depends on your region.

- If you have the login and password for your My Kaspersky account, enter your credentials and click **Sign In**.

Note: If you enter the password incorrectly several times in a short period, you will need to enter characters from a picture to pass the security check.

Note: If you have [enabled two-step verification for your My Kaspersky account](#), you will need to enter a code received via an SMS message or generated in an authenticator app.

A dialog with the Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement) opens.

3. Do one of the following:

- If you don't accept the Web-Portal Statement, click **Decline**.

Note: You can't sign in to My Kaspersky or create a My Kaspersky account without accepting the Web-Portal Statement.

- If you accept the Web-Portal Statement, click **Accept** to continue.

Kaspersky VPN signs you in to the My Kaspersky account.

[Create a My Kaspersky account from the application interface](#)

1. In the **Sign In to My Kaspersky** window, click **Create Account**.

The **Create a My Kaspersky Account** window opens.

Note: If you enter an email address that is already in use, an incorrect email address, or a too common password several times in a short period, you will need to enter characters from a picture to pass the security check.

2. In the email address field, enter the email address that you want to associate with your new My Kaspersky account.

3. In the password field, enter the password for your new My Kaspersky account.

Note: The password must contain a minimum of eight characters, including at least one digit, one lowercase letter, and one uppercase letter. Spaces are not allowed.

4. In the password confirmation field, enter the password again.

5. In the country selection pop-up menu, select your country.

Note: Kaspersky VPN automatically displays your country, based on the region set in your system's Language & Region settings. This option determines the regional settings for your My Kaspersky account, for example, the display language and available Kaspersky applications. You can change your region for My Kaspersky later only by contacting Customer Service.

6. Click the **Privacy Policy** link to read the Privacy Policy, which describes how data is handled.

A browser window with the Privacy Policy opens.

7. If you agree with the terms of the Privacy Policy, select the **I confirm that I have fully read, understand, and accept the terms and conditions of the Privacy Policy describing the handling of data** checkbox.

Note: The **Create** button becomes available only if you confirm that you have fully read, understand, and accept the Privacy Policy.

8. If you agree to provide Kaspersky with your email address for receiving informational and promotional email messages, select the **I agree to provide Kaspersky with my email address to receive personalized marketing offers** checkbox.

9. Click **Create**.

A dialog with the Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement) opens.

10. Do one of the following:

- If you don't accept the Web-Portal Statement, click **Decline**.

Note: You can't sign in to My Kaspersky or create a My Kaspersky account without accepting the Web-Portal Statement.

- If you accept the Web-Portal Statement, click **Accept** to continue.

Kaspersky VPN connects to My Kaspersky and creates your account. After your account is created, the main application window opens and an email message with instructions on account activation is sent to the email address that you specified during registration.

Important: Internet access is required to connect to My Kaspersky.

Kaspersky VPN versions

Kaspersky VPN is available in free and Unlimited versions.

Free version:

- Free of charge.
- Always available.
- Limited amount of secure traffic per day.
- You can't choose the VPN server. It is selected automatically.

You can [switch from the free version to the Unlimited version](#) by purchasing a subscription.

Unlimited version:

- Unlimited daily traffic.
- You can [choose the VPN server](#).
- [Kill Switch](#).
- Available via a subscription.
- The application may be installed on several devices (Mac, mobile, tablet, PC) under one subscription.

For more information on Kaspersky VPN versions, visit [My Kaspersky](#).

Note: When you use the Unlimited version of Kaspersky VPN, the application may notify you that another subscription is available. This notification appears only if the found subscription applies to fewer devices than your current subscription. If you switch to this subscription, Kaspersky VPN installed on some of your devices will switch to the free version.

Note: [The application will stop working in Russia](#).

Upgrade to the Unlimited version

If you want unlimited secure traffic and freedom to choose VPN servers, you can upgrade to the Unlimited version of Kaspersky VPN. If you have already been using the Unlimited version and your subscription has expired or the grace period has started, you can renew it.

[Buy/renew a subscription](#)

1. In the traffic or subscription card of the main application window, click **Upgrade** or **Details**.

A window with the current subscription status opens.

2. Follow the instructions on the screen to buy or renew a subscription.

Note: If you are not connected to My Kaspersky, Kaspersky VPN displays the Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement) before you can buy a subscription. Please note that, by purchasing the subscription, you confirm that you have fully read, understand, and accept the Purchase Statement.

You can also buy a subscription for Kaspersky VPN on [My Kaspersky](#)  or on the [Kaspersky website](#) .

- If you purchase the subscription on My Kaspersky, the subscription will be activated automatically as soon as you complete the purchase.
- If you purchase the subscription on the Kaspersky website, you will receive an activation code in an email sent to the email address you specified. To activate the subscription, you need to add the activation code to your My Kaspersky account and [connect Kaspersky VPN to My Kaspersky](#). For detailed information on how to manually add your activation code to your My Kaspersky account, see the [My Kaspersky help](#) .

Protect your connection to an unsecured Wi-Fi network

When joining any Wi-Fi network, Kaspersky VPN checks the status of the Wi-Fi network in accordance with data from Kaspersky Security Network and other criteria such as whether a vulnerable encryption protocol or a common network name (SSID) are used. Using this information, Kaspersky VPN determines whether or not the Wi-Fi network is secure.

If you have already connected to an unsecured Wi-Fi network, you can protect your connection using Kaspersky VPN.

[Protect your connection to an unsecured Wi-Fi network](#)

1. In the main application window, turn VPN on.
2. In the alert that appears, click **Yes, Turn On**, if you want Kaspersky VPN to turn on VPN automatically when joining an unsecured Wi-Fi network.

[Enable detection of unsecured Wi-Fi networks with Kaspersky Security Network](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Unsecured Wi-Fi** tab, select the **Enable cloud detection with Kaspersky Security Network** checkbox.

A window with instructions opens.

Note: macOS requires Location Services to be enabled for Kaspersky VPN to obtain a Wi-Fi network name (BSSID). Kaspersky Security Network will use this to detect unsecured Wi-Fi networks. It won't be used to determine your real location.

3. Follow the instructions on the screen.

The application will use Kaspersky Security Network to detect unsecured Wi-Fi networks.

Why is it impossible to open a website with Kaspersky VPN enabled?

Some websites and web services deny access when you try to connect to them through a VPN. Websites and web services may deny VPN access for the following reasons:

- Website owners want the licensed content they publish to only be available for a certain country, since there are different offers and prices for different countries.
- Website owners want the website to only be visited from a certain region. For example, a lottery is drawn only for a certain country, so access from other regions is forbidden.
- There are web services that, for legal reasons, are only available in a particular region (for example, some media services providers or news broadcasters). These web services resist anonymizers and are not available when you use a VPN (or another anonymizer) to reach them.
- These web services not only determine the location of the client, but also determine if the client uses an anonymizer. If an attempt to access the web service via an anonymizer is detected, access to the web service is blocked.
- If you cannot access a certain website or web service by using a Kaspersky VPN, we recommend [contacting Customer Service](#). Report the web service that is unavailable and from which location. Kaspersky will do our best to resolve the issue.

Subscription & account

Kaspersky VPN versions

Kaspersky VPN is available in free and Unlimited versions.

Free version:

- Free of charge.
- Always available.
- Limited amount of secure traffic per day.
- You can't choose the VPN server. It is selected automatically.

You can [switch from the free version to the Unlimited version](#) by purchasing a subscription.

Unlimited version:

- Unlimited daily traffic.
- You can [choose the VPN server](#).
- [Kill Switch](#).
- Available via a subscription.
- The application may be installed on several devices (Mac, mobile, tablet, PC) under one subscription.

For more information on Kaspersky VPN versions, visit [My Kaspersky](#).

Note: When you use the Unlimited version of Kaspersky VPN, the application may notify you that another subscription is available. This notification appears only if the found subscription applies to fewer devices than your current subscription. If you switch to this subscription, Kaspersky VPN installed on some of your devices will switch to the free version.

Note: [The application will stop working in Russia](#).

Upgrade to the Unlimited version

If you want unlimited secure traffic and freedom to choose VPN servers, you can upgrade to the Unlimited version of Kaspersky VPN. If you have already been using the Unlimited version and your subscription has expired or the grace period has started, you can renew it.

[Buy/renew a subscription](#)

1. In the traffic or subscription card of the main application window, click **Upgrade** or **Details**.

A window with the current subscription status opens.

2. Follow the instructions on the screen to buy or renew a subscription.

Note: If you are not connected to My Kaspersky, Kaspersky VPN displays the Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement) before you can buy a subscription. Please note that, by purchasing the subscription, you confirm that you have fully read, understand, and accept the Purchase Statement.

You can also buy a subscription for Kaspersky VPN on [My Kaspersky](#) or on the [Kaspersky website](#):

- If you purchase the subscription on My Kaspersky, the subscription will be activated automatically as soon as you complete the purchase.
- If you purchase the subscription on the Kaspersky website, you will receive an activation code in an email sent to the email address you specified. To activate the subscription, you need to add the activation code to your My Kaspersky account and [connect Kaspersky VPN to My Kaspersky](#). For detailed information on how to manually add your activation code to your My Kaspersky account, see the [My Kaspersky help](#).

Restore your subscription

When you [sign in to your My Kaspersky account](#), the details of your subscription automatically appear on [My Kaspersky](#). If you want to apply this subscription to Kaspersky VPN installed on another Mac device, you only need to sign in to My Kaspersky.

If you haven't signed in to My Kaspersky and you want to apply your subscription to the free version of Kaspersky VPN on another Mac device, you may need to restore your subscription.

[Restore your subscription](#)

1. Open the main application window on a device with the free version of Kaspersky VPN installed.
2. In the traffic card of the main application window, click **Upgrade**.
A window with the current subscription status opens.
3. Click **Restore Purchases**.
A dialog with the Purchase Statement appears.

Note: After clicking **Restore Purchases**, you may have to restart the application.

4. Click **Accept**.
5. In the prompt for your App Store credentials, enter your login and password.

Your subscription is applied to Kaspersky VPN.

Change the My Kaspersky account

If you want to use a different My Kaspersky account, you can sign out of the current My Kaspersky account from the application interface and sign in to another My Kaspersky account.

[Change the My Kaspersky account](#)

1. In the lower-left corner of the main application window, click your email address.
2. In the dialog that opens, click **Sign Out**.
3. In the **You will be signed out of My Kaspersky** dialog, click **Sign Out** to confirm that you want to sign out of your current My Kaspersky account.
The **Sign In to My Kaspersky** window opens.
4. Enter the credentials of another My Kaspersky account and click **Sign In**.

About the subscription

A *subscription for Kaspersky VPN* is the purchase of the right to use the application according to specific parameters (for example, subscription expiration date, number of devices). You can order a subscription for Kaspersky VPN from a service provider (for example, on Google Play or the App Store).

You can manage your subscription via your personal account page on the service provider's website (for example, via your Apple account or Google Account).

Before buying a subscription, you can try the Unlimited version of Kaspersky VPN free of charge. The trial subscription for Kaspersky VPN remains functional during a short trial period. When the trial period ends, you will be charged for a subscription. If you do not want to use Kaspersky VPN, you must cancel the subscription before the trial period ends.

A subscription can be renewed automatically or manually. An auto-renewed subscription automatically renews at the end of each subscription period until you cancel it. A manually renewed subscription must be renewed at the end of each subscription period. After your subscription for Kaspersky VPN expires, you may be offered a grace period, during which you can continue using the application without limitations. If you don't renew your subscription by the end of the grace period, the application will switch to the free version. To switch back to the Unlimited version, buy a new subscription.

Important: Ordering a subscription for Kaspersky VPN does not cancel your other subscriptions that include Kaspersky VPN. To avoid additional charges, make sure you have canceled or disabled autorenewal for subscriptions that you don't need.

Cancel a subscription for Kaspersky VPN or switch to manual renewal:

1. Go to your personal account page on the service provider's website.
2. Check if there are any active subscriptions that include Kaspersky VPN.
3. Cancel or disable autorenewal for subscriptions that you don't need.

About anonymous subscriptions

Your subscription is considered "anonymous" if you purchased a subscription for the Unlimited version of Kaspersky VPN from the App Store while not signed in to your My Kaspersky account or when you didn't have a My Kaspersky account. An anonymous subscription is associated with your App Store account, but not with your My Kaspersky account.

You can associate your anonymous subscription with your My Kaspersky account at any time. After you [sign in to My Kaspersky](#) on the device with the Unlimited version of Kaspersky VPN, your subscription is automatically associated with your My Kaspersky account. This process may take some time, and active VPN sessions on your devices may be stopped. After that, you can use My Kaspersky to manage your subscription. All devices that use this subscription will be automatically connected to your My Kaspersky account. You will also be able to use your My Kaspersky account to apply your subscription to Kaspersky VPN on new devices (if the device limit has not been reached).

When you restore an anonymous subscription from Kaspersky VPN while signed in to your My Kaspersky account, your subscription is automatically associated with your My Kaspersky account as well. All devices that use this subscription will be automatically connected to it.

Note: After your subscription is associated with your My Kaspersky account, you need to confirm all your automatically connected devices on My Kaspersky.

You can disconnect the subscription from My Kaspersky by contacting Customer Service.

[Disconnect an anonymous subscription from your device](#) 

1. Click **Subscription Details**.

A window with the current subscription details appears.

2. Click **Disconnect from Subscription**.

3. Confirm the action by clicking **Disconnect from Subscription** again.

Your application switches to the free version.

Data provision

About data provided

[View information about the data provided to Kaspersky while using previous versions of the application](#) 

- [Kaspersky VPN 2.16](#) 
- [Kaspersky VPN 2.15](#) 
- [Kaspersky VPN 2.14](#) 
- [Kaspersky VPN 2.13](#) 
- [Kaspersky VPN 2.12](#) 
- [Kaspersky VPN 2.11](#) 
- [Kaspersky VPN 2.10](#) 
- [Kaspersky VPN 2.9](#) 
- [Kaspersky VPN 2.8](#) 
- [Kaspersky VPN 2.7](#) 
- [Kaspersky VPN 2.6](#) 
- [Kaspersky Secure Connection 2.5](#) 
- [Kaspersky Secure Connection 2.4](#) 
- [Kaspersky Secure Connection 2.3](#) 
- [Kaspersky Secure Connection 2.2](#) 
- [Kaspersky Secure Connection 2.1](#) 
- [Kaspersky Secure Connection 2.0](#) 
- [Kaspersky Secure Connection 1.0](#) 

Data provided to Kaspersky by using Kaspersky VPN 3.0

Kaspersky protects any information received in accordance with law and applicable Kaspersky rules. Data is transmitted over a secure channel.

Personal data provided

You agree to provide Kaspersky with personal data by accepting the End User License Agreement, Privacy Policy, Statement Regarding Data Processing For Marketing Purposes (Marketing Statement), Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement), or Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement). You can view the list of data provided under the terms of each legal document in the corresponding legal document.

You can view the License Agreement in the App Store.

[Read the Marketing Statement and disable sending data](#) ⓘ

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Improved experience** section, click **Show Marketing Statement** if you want to read the terms of the Marketing Statement.

A window with the Marketing Statement opens.

3. If you want to disable sending data, deselect the **Help Kaspersky improve its products by sending information about the application and its operating environment** checkbox.

If you don't want Kaspersky to receive and process the data provided under the Purchase Statement, you can revoke your acceptance by disconnecting your subscription.

[Disconnect an anonymous subscription from your device](#) ⓘ

1. In the subscription card of the main application window, click **Details**.

A window with the current subscription status opens.

2. Click **Subscription Details**.

A window with the current subscription details appears.

3. Click **Disconnect from Subscription**.

4. Confirm the action by clicking **Disconnect from Subscription** again.

Your application switches to the free version.

Important: After you disconnect Kaspersky VPN from the subscription, the subscription remains active. For more information about the subscription terms, see [About the subscription](#).

If you don't want Kaspersky to receive the data provided under the Web-Portal Statement, you can revoke your acceptance signing out of [My Kaspersky](#) ⓘ.

[Sign out of My Kaspersky](#) ⓘ

1. In the lower-left corner of the main application window, click your email address.
2. In the dialog that opens, click **Sign Out**.

If you don't want Kaspersky to process the data provided under the Web-Portal Statement, you need to delete your My Kaspersky account.

[Delete your My Kaspersky account](#)

1. In the lower-left corner of the main application window, click your email address.
2. In the dialog that opens, click **Delete Account**.
A browser window opens.
3. Follow the instructions in the browser.

For more information about deleting a My Kaspersky account, see the [My Kaspersky help](#) .

Important: When you sign out of or delete a My Kaspersky account, Kaspersky VPN switches to the free version.

Non-personal data provided

You agree to provide Kaspersky with non-personal data by accepting the End User License Agreement.

Non-personal data is provided to Kaspersky for the following purposes:

To provide You with the core functionality of the acquired Rightholder's Software.

- Information about the Rightholder's Software: full version of the Software; Software ID; Software localization; Software group; the result of the Software action; error code.
- Information about the use of Kaspersky Security Network (KSN): the configuration identifier.
- Reason for VPN session interruption; VPN session duration; ID of the topic in the Software help; link name.

In addition to the information mentioned above, in case of signing in to the Web-Portal using Your Facebook or Google account, the Rightholder needs to receive from Your device and process the following non-personal data:

- Information about the authentication: authorization code received from the identity provider; access token received from the identity provider; type of data sent to the identity provider; Rightholder ID in the identity provider's system; name of the identity provider; URI to which the identity provider's response is sent; parameters requested from the identity provider; ID of the Rightholder's resource; token type; value generated for request verification.

Note: The availability of the option to sign in with Facebook depends on your region.

To improve the quality, appearance, and performance of the Rightholder's Software, products, services, and infrastructure by analyzing users' interactions, experience, and satisfaction.

- Information about the End User's Computer on which the Software is installed: device model; OS build number; extended information about the OS edition; operating system family; OS Service Pack version; version of the operating system installed on the user's computer; operating system bit version; OS edition; device type (laptop, desktop, tablet); OS type (server, workstation, domain controller); country code.
- Information about the Rightholder's Software: statistics submission scenario; Software operating mode; information about VPN nodes; full version of the Software; Software update ID; Software ID; Software localization; Software rebranding ID; type of the installed Software; the result of the Software action; error code; Software installation/uninstallation status; installation error code; flag indicating whether the installation was aborted by the user; duration of Software installation in seconds; installation type (new installation, update); operating mode of Kaspersky VPN Secure Connection; ID of the starting scenario of VPN connection; status of VPN client settings; Software IDs in Firebase.
- Information about the use of Kaspersky Security Network (KSN): protocol used to exchange data with KSN; ID of the KSN service accessed by the Software; date and time when statistics stopped being received; number of KSN connections taken from the cache; number of requests for which a response was found in the local request database; number of unsuccessful KSN connections; number of unsuccessful KSN transactions; temporal distribution of cancelled requests to KSN; temporal distribution of unsuccessful KSN connections; temporal distribution of unsuccessful KSN transactions; temporal distribution of successful KSN connections; temporal distribution of successful KSN transactions; temporal distribution of successful requests to KSN; temporal distribution of requests to KSN that timed out; number of new KSN connections; number of unsuccessful requests to KSN caused by routing errors; number of unsuccessful requests caused by KSN being disabled in the Software settings; number of unsuccessful requests to KSN caused by network problems; number of successful KSN connections; number of successful KSN transactions; total number of requests to KSN; date and time when statistics started being received.
- Authorization code received from the identity provider; access token received from the identity provider; type of data sent to the identity provider; Rightholder ID in the identity provider's system; name of the identity provider; URI to which the identity provider's response is sent; parameters requested from the identity provider; text of the error message; OS error code; reason for VPN session interruption; VPN session duration; http request method; ID of the Rightholder's resource; token type; authentication token in the Rightholder's services; token TTL; path to the object being processed; method used for authentication in the Software; value generated for request verification; ID of the topic in the Software help; information about implementation of the web service access handler; unique request ID to the Rightholder services; link name; line number of the source file in the exception handler; volume of inbound traffic; volume of outbound traffic; protocol ID; total duration of request processing; protocol processing error type; exit country of VPN traffic; code of the error category; DNS address of the web service being accessed; server access duration; remote port and IP address of the web service being accessed; web address being processed.

Compliance with European Union law

When distributed in the European Union, Kaspersky VPN complies with the terms of the General Data Protection Regulation (GDPR).

When you accept the End User License Agreement, you confirm that you are of the required age to install Kaspersky VPN within the European Union territory. After Kaspersky VPN is installed, you will be asked to read and accept the terms and conditions required for initial setup and use of Kaspersky VPN: the Conditions Regarding Data Processing and the Privacy Policy and the Statement Regarding Data Processing For Marketing Purposes (Marketing Statement).

Also you will be asked to read and accept the terms and conditions required for use of Kaspersky VPN: Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement) and Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement).

If you choose to accept these statements, you can still revoke your acceptance in the application settings at any time.

Important: If you have an earlier version of Kaspersky VPN installed on OS X 10.11 (El Capitan) and you intend to use the application within the European Union, then you should upgrade your operating system to macOS 10.14 and then upgrade Kaspersky VPN. If you do not want to upgrade your operating system right away, remove Kaspersky VPN from your computer.

Contents of trace files, dump files, and settings files

Note: All files described in this section can be accessed only by the system administrator of the computer and the owner of the computer account with Kaspersky VPN installed.

1. Trace files

Trace files contain information about events that occur during the operation of Kaspersky VPN. Trace files are stored locally on your computer in the following folder: `~/Library/Group Containers/2Y8XE5CQ94.com.kaspersky.ksec/Library/Application Support/KSEC/Logs/`

Traces are contained in the following files:

- `ksec_agent_<timestamp>.log`
- `ksec_app_<timestamp>.log`
- `ksec_daemon_<timestamp>_pid_<PID>.log`
- `ksec_networkextension_<timestamp>.log`

Trace files may contain the following information:

- Information about the device and operating system (unique device ID, device type, MAC addresses of network devices, operating system type, operating system version)
- Information about applications being loaded by the user (URL, attributes, file size, information about the process that loaded the file)
- Information about launched applications and their modules
- Information about the operation of the application and its modules
- Information about errors in and the use of the graphical user interface of the installed Kaspersky application
- Information about network connections and network settings: the IP address of the remote computer and the user's computer, the IP address of DNS servers, MAC address of the access point, network name, signal strength, port numbers of ports used to establish the connection, network protocol, connection status at time of file generation, network reputation, proxy server settings – the user name/password hash
- Information about settings for connecting to Kaspersky servers

- Information about connections to Aura servers
- Information about the license type (license type, region)
- Information about network packets received and sent by the computer over the telecommunications network
- Information about sent and received emails and instant messages
- Information about My Kaspersky: information about the website user names and passwords, and contents of cookie files
- Server's public certificate
- Information about the language locale, software ID, software customization, software version, unique software installation ID, unique computer ID

Trace files contain only the information necessary to fix defects in the application. Kaspersky uses trace files to investigate incidents associated with errors in the operation of Kaspersky VPN.

By default, the creation of trace files is disabled. You can enable generation of trace files in the application settings.

Trace files can only be sent to Kaspersky manually. Kaspersky VPN does not send trace files to Kaspersky automatically.

You can choose how trace files are sent to Kaspersky.

Before sending trace files to Kaspersky, please review their contents.

Important: Trace files may contain personal or sensitive information. By sending trace files to Kaspersky, you agree to provide to Kaspersky all data contained in the trace files you send, and you consent to the method used to send them.

2. Dump files

Dump files contain all information about the working memory of the application's processes at the time the dump is created. Dump files may contain confidential data.

Dump files are generated by the operating system and are sent to Apple servers only with your consent. Before sending a dump file, please review its contents.

3. Additional files

In addition, Kaspersky VPN generates additional settings files that are stored on the user computer. These files may contain information necessary for operation of the Software: settings, internal databases, configuration files.

Customer Service specialists might ask you to provide the additional files in order to shorten the time required to process requests associated with errors in the Software. The user sends this data manually at the request of a Customer Service specialist.

By sending the additional settings files to Customer Service, you agree to provide all data they contain and you consent to the method used to send them. Before sending these files, please review their contents.

These additional files may contain the following information:

- Proxy server settings – the user name and password hash
- Credentials for connecting to My Kaspersky
- Names of Wi-Fi networks for which the rules of enabling secure connection are configured

Get started with the application

Hardware and software requirements

Kaspersky VPN has the following hardware and software requirements:

- 1 GB of memory (RAM)
- 320 MB of free disk space
- Operating system macOS 11-13
- Internet connection
- Processor type: Intel, Apple silicon

Install and uninstall the application

You can install Kaspersky VPN from the App Store.

To install the application:

1. Open the App Store application.
2. Find Kaspersky VPN and install the application.

The App Store may prompt you to enter your Apple ID credentials.

Note: For more information on using the App Store and installing applications, refer to the relevant user guides for your Mac.

To uninstall the application:

1. Locate the application in the Finder.
2. Open the shortcut menu and choose **Move to Trash**.

Note: For more information on uninstalling applications, refer to the relevant user guides for your Mac.

Start the application for the first time

When you start Kaspersky VPN on your computer for the first time, the application prompts you to accept the terms and conditions required for initial setup and use of Kaspersky VPN.

Start Kaspersky VPN for the first time 

1. Click the Launchpad icon in the Dock.

A window with the list of applications opens.

2. Click the Kaspersky VPN icon.

3. In the **Before you start, please review the Conditions Regarding Data Processing and the Privacy Policy** window, read the text of the Conditions Regarding Data Processing.

4. Click the **Privacy Policy** link to read the Privacy Policy, which describes how data is handled.

A browser window with the Privacy Policy opens.

5. Do one of the following:

- If you don't agree with the Conditions Regarding Data Processing or the Privacy Policy, close the application window and don't use the application.
- If you agree with the Conditions Regarding Data Processing and the Privacy Policy, confirm that by selecting the appropriate checkboxes.

Note: The **Accept** button becomes available only if you confirm that you have fully read, understand, and accept both the Conditions Regarding Data Processing and the Privacy Policy.

6. Click **Accept**.

7. In the **Statement regarding data processing for marketing purposes** window, read the text of the Marketing Statement. By accepting the Marketing Statement, you allow Kaspersky to offer you additional benefits.

8. If you agree with the terms of the Statement Regarding Data Processing For Marketing Purposes, click **Accept** and then in the confirmation dialog that appears, click **Confirm**.

Note: You can revoke your acceptance in the application settings at any time.

9. In the next window, you can get the Unlimited version of Kaspersky VPN. Do one of the following:

- If you want to start your 7-day free trial or subscribe, click the blue button with the corresponding text. By clicking **Start 7-Day Free Trial** or **Subscribe for <price>/year**, or **Subscribe for <price>/month**, you confirm that you have fully read, understand, and accept the terms of the Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement) usually displayed to the right of the application window.
- If you have previously purchased a subscription for Kaspersky VPN and want to apply this subscription to this copy of the application, click **Restore Purchases** in the upper-right corner of the application window.

If you haven't accepted the Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement) before, view the terms of this statement in the dialog that opens and click **Accept**. By clicking **Accept**, you confirm that you have fully read, understand, and accept the Statement Regarding Data Processing For Purpose Of Completing A Purchase (Purchase Statement).

Note: You can skip this step by clicking **Skip**. You will proceed with the free version of Kaspersky VPN. You can get the Unlimited version of the application later, at any time.

The main application window opens.

Connect to My Kaspersky

When you open Kaspersky VPN, you can sign in to [My Kaspersky](#) with a [My Kaspersky account](#). If you have used another Kaspersky application, for example, Kaspersky VPN for another device or Kaspersky Internet Security, you probably already have a My Kaspersky account. Use it to sign in. If you don't have an account, you can create one.

Note: If you have signed in to My Kaspersky in another Kaspersky application on your Mac, the Kaspersky VPN application prompts you to sign in to My Kaspersky using the same account after the application installation.

[Sign in to My Kaspersky using your existing account](#)

1. Open the main application window and click **Sign In**.

The **Sign In to My Kaspersky** window opens.

2. Do one of the following:

- If you want to connect to My Kaspersky with your Google, Facebook, or Apple account, click the corresponding button and follow the instructions. For more details, see the [My Kaspersky help](#). If you don't have a My Kaspersky account yet, the application will prompt you to register on My Kaspersky.

Note: The availability of the option to sign in with Facebook depends on your region.

- If you have the login and password for your My Kaspersky account, enter your credentials and click **Sign In**.

Note: If you enter the password incorrectly several times in a short period, you will need to enter characters from a picture to pass the security check.

Note: If you have [enabled two-step verification for your My Kaspersky account](#), you will need to enter a code received via an SMS message or generated in an authenticator app.

A dialog with the Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement) opens.

3. Do one of the following:

- If you don't accept the Web-Portal Statement, click **Decline**.

Note: You can't sign in to My Kaspersky or create a My Kaspersky account without accepting the Web-Portal Statement.

- If you accept the Web-Portal Statement, click **Accept** to continue.

Kaspersky VPN signs you in to the My Kaspersky account.

[Create a My Kaspersky account from the application interface](#)

1. In the **Sign In to My Kaspersky** window, click **Create Account**.

The **Create a My Kaspersky Account** window opens.

Note: If you enter an email address that is already in use, an incorrect email address, or a too common password several times in a short period, you will need to enter characters from a picture to pass the security check.

2. In the email address field, enter the email address that you want to associate with your new My Kaspersky account.
3. In the password field, enter the password for your new My Kaspersky account.

Note: The password must contain a minimum of eight characters, including at least one digit, one lowercase letter, and one uppercase letter. Spaces are not allowed.

4. In the password confirmation field, enter the password again.
5. In the country selection pop-up menu, select your country.

Note: Kaspersky VPN automatically displays your country, based on the region set in your system's Language & Region settings. This option determines the regional settings for your My Kaspersky account, for example, the display language and available Kaspersky applications. You can change your region for My Kaspersky later only by contacting Customer Service.

6. Click the **Privacy Policy** link to read the Privacy Policy, which describes how data is handled.

A browser window with the Privacy Policy opens.

7. If you agree with the terms of the Privacy Policy, select the **I confirm that I have fully read, understand, and accept the terms and conditions of the Privacy Policy describing the handling of data** checkbox.

Note: The **Create** button becomes available only if you confirm that you have fully read, understand, and accept the Privacy Policy.

8. If you agree to provide Kaspersky with your email address for receiving informational and promotional email messages, select the **I agree to provide Kaspersky with my email address to receive personalized marketing offers** checkbox.

9. Click **Create**.

A dialog with the Statement Regarding Data Processing For Purpose Of Using Web-Portal (Web-Portal Statement) opens.

10. Do one of the following:

- If you don't accept the Web-Portal Statement, click **Decline**.

Note: You can't sign in to My Kaspersky or create a My Kaspersky account without accepting the Web-Portal Statement.

- If you accept the Web-Portal Statement, click **Accept** to continue.

Kaspersky VPN connects to My Kaspersky and creates your account. After your account is created, the main application window opens and an email message with instructions on account activation is sent to the email address that you specified during registration.

Important: Internet access is required to connect to My Kaspersky.

About two-step verification

Important: Two-step verification may be unavailable in your region. For more details, see the [My Kaspersky help](#).

Two-step verification prevents bad guys from signing in to your My Kaspersky account even if they know your password. To verify your identity, you will receive a unique security code in one of the following ways:

- Via an SMS. We use the phone number you save on My Kaspersky. This means that both your password and your phone are needed to sign in to your account.
- Via an authenticator app. You first need to set up two-step verification via your mobile phone number for the authenticator app feature to be available.

You can turn on two-step verification on My Kaspersky. If you change your phone number, you can update it on [My Kaspersky](#). If you are already signed in to your account on a device, nothing will change for you. For detailed instructions, see the [My Kaspersky help](#).

Note: The security code is valid for a short period. If it expires, request another security code.

If you haven't received an SMS message with a security code

1. Check whether your mobile device is turned on and your mobile network is available.
2. Wait until the **Request Code Again** button becomes available.
3. Click **Request Code Again**.

If the problem still persists, contact Customer Service.

Perform common tasks

Activate VPN connection

Use one of the following methods to activate a secure connection in Kaspersky VPN:

1. You can turn VPN on/off from the application interface or in the menu bar.

Note that when you quit Kaspersky VPN, the application stops running and the secure connection turns off.

[Turn VPN on ?](#)

Do one of the following:

- In the main application window, turn on VPN.
- In the menu bar, click the application icon and choose **Turn VPN On**.

[Turn VPN off ?](#)

Do one of the following:

- In the main application window, turn off VPN.
- In the menu bar, click the application icon and choose **Turn VPN Off**.

2. You can let Kaspersky VPN run in the background.

If this option is enabled, the application will always monitor your Wi-Fi connections and warn you if you join an unsecured Wi-Fi network. You can set up Kaspersky VPN to [automatically turn VPN on when an unsecured network is detected](#). We recommend using this option.

If you want to stop the application, you can quit it manually.

[Let Kaspersky VPN run in the background ?](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Run in background** section, select the **Let Kaspersky VPN run in the background (recommended)** checkbox.

When you quit Kaspersky VPN, the application will continue running in the background.

[Quit Kaspersky VPN from the application icon menu ?](#)

In the menu bar, click the application icon and choose **Quit** or **Disconnect and Quit**, when Kaspersky VPN runs in the background.

3. For maximum protection, you can set Kaspersky VPN to automatically turn VPN on when your Mac starts.

[Let Kaspersky VPN automatically protect your connection ?](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Run in background** section, select the **Let Kaspersky VPN run in the background (recommended)** checkbox and then select the **Turn on VPN automatically when your Mac starts** checkbox.

Note: The **Turn on VPN automatically when your Mac starts** checkbox is available if the **Let Kaspersky VPN run in the background (recommended)** checkbox is selected.

Note: A secure connection can be lost due to an unstable internet connection or when switching between networks. In this case, the transmitted data is not protected. Kaspersky VPN restores the secure connection after reconnecting to the internet. If the secure connection cannot be restored, Kaspersky VPN will notify you. To protect your data if the secure connection is lost, you can use Kill Switch. It completely blocks the transfer of data until the secure connection is restored.

Select a VPN server

If you want to hide your IP address and appear to the internet as a visitor from a different place, you can change your location by selecting a different VPN server. [Kaspersky VPN at the moment supports the following VPN server locations](#).

If you want to view a movie or show on the day of its world premiere even though it is scheduled for a later date in your specific region, all you need to do is start the application and select a region where it is available. [We recommend the following servers for regional content](#).

Note: The locations in the list are determined based on the VPN server's IP address and don't necessarily match the physical location of the VPN server.

[Select a VPN server](#)

1. In the VPN server card of the main application window, click **Change**.

A list of VPN servers opens.

2. Select the VPN server that you want to use.

Kaspersky VPN connects the selected VPN server right away.

Note: Only the Unlimited version of the application allows you to select the VPN server that you want to use. In the free version, Kaspersky VPN selects the location of your free VPN server automatically.

View the amount of used and available traffic

Kaspersky VPN displays the amount of used and available traffic in the free version of the application.

If you are using the free version of Kaspersky VPN, your use of secure traffic is limited each day. If you exceed your limit on secure traffic, the application notifies you that a secure connection is unavailable. It may take several minutes after the notification is displayed before your secure connection is actually disabled.

You can remove the limitation by [upgrading to the Unlimited version of the application](#).

[View the amount of used and available traffic](#)

Open the main application window and view the traffic card in the lower-right corner.

Note: You can also view the amount of used and available traffic in the application's **Connection** menu or in the application icon menu.

Information about available and used traffic is updated no more than once per minute. After a secure connection is disabled, information about used secure traffic is updated within 30 seconds.

How to configure Split Tunneling

You can configure enabling a VPN connection only for selected applications (Split Tunneling).

[Turn on VPN only for selected apps](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Split Tunneling** tab, select the **Turn on VPN only for selected apps** checkbox.

3. Do one of the following:

- To add an application to the list, type or select an app name in the selection field.
- To remove an application from the list, select it and click .

Note: Split Tunneling is available only in the Unlimited version of Kaspersky VPN.

Protect your data if your secure connection is lost

When you turn on VPN, your data is reliably protected while you surf the internet. However, if the VPN connection drops, your data will be unprotected, and attackers can steal it. To ensure that your data is always protected, you can use *Kill Switch*. Kill Switch will cut off data transfer over the internet when VPN is reconnecting. Your internet connection will be restored as soon as VPN turns on.

Important: To protect your data, Kill Switch blocks data transfer via the internet entirely, until VPN is restored. This doesn't affect data transfer on your local network. Your Mac can interact with other devices in your local network without any limitations.

By default, Kill Switch is turned off and Kaspersky VPN does not block your internet access if the VPN connection is interrupted.

[Turn on Kill Switch](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Kill Switch** tab, select the **Turn on Kill Switch** checkbox.

A window with the information about Kill Switch opens.

3. Click **Turn On Anyway**.

The application will block your internet access if the VPN connection is interrupted.

Note: Kill Switch is available only in the Unlimited version of Kaspersky VPN.

Set up VPN settings for known Wi-Fi networks

If you regularly connect your Mac to a specific Wi-Fi network, you can configure VPN settings for that network.

[Configure VPN settings for a specific Wi-Fi network](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Unsecured Wi-Fi** tab, select the action to perform upon connecting to the Wi-Fi network for which you want to configure VPN settings:

- **Not Specified.** If the specified Wi-Fi network is unsecured, the application applies the settings specified for unsecured Wi-Fi networks. If the specified network is secure, the application does nothing.
- **Turn VPN On.** The application turns on VPN when you connect your Mac to the specified Wi-Fi network.
- **No Action.** The application does not turn on VPN when you connect your Mac to the specified Wi-Fi network.

Enable or disable sending data for marketing purposes

You can enable or disable sending data that helps Kaspersky improve the quality, appearance, and performance of its applications. You can learn what kind of data is sent to Kaspersky by reading the Marketing Statement.

[View the Marketing Statement](#) ⓘ

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Improved experience** section, click **Show Marketing Statement**.

A window with the Marketing Statement opens.

[Enable or disable sending data for marketing purposes](#) ⓘ

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Improved experience** section, do one of the following:

- If you want to enable sending data, select the **Help Kaspersky improve its products by sending information about the application and its operating environment** checkbox and click **Confirm** in the dialog that opens.
- If you want to disable sending data, deselect the **Help Kaspersky improve its products by sending information about the application and its operating environment** checkbox.

Enable tracing

Tracing is a way to record detailed information about the application's activity. Kaspersky Customer Service specialists use trace files to troubleshoot issues. You can enable application event logging to create trace files and send them to Customer Service if requested. By default, application event logging is disabled.

[Enable logging of data to trace files](#) 

1. Open Kaspersky VPN.
2. In the menu bar, choose **Help > Enable Tracing**.

Important: Turn on tracing only when a Customer Service specialist asks you to do so.

Protect your connection to an unsecured Wi-Fi network

When joining any Wi-Fi network, Kaspersky VPN checks the status of the Wi-Fi network in accordance with data from Kaspersky Security Network and other criteria such as whether a vulnerable encryption protocol or a common network name (SSID) are used. Using this information, Kaspersky VPN determines whether or not the Wi-Fi network is secure.

If you have already connected to an unsecured Wi-Fi network, you can protect your connection using Kaspersky VPN.

[Protect your connection to an unsecured Wi-Fi network](#) 

1. In the main application window, turn VPN on.
2. In the alert that appears, click **Yes, Turn On**, if you want Kaspersky VPN to turn on VPN automatically when joining an unsecured Wi-Fi network.

[Enable detection of unsecured Wi-Fi networks with Kaspersky Security Network](#) 

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Unsecured Wi-Fi** tab, select the **Enable cloud detection with Kaspersky Security Network** checkbox.

A window with instructions opens.

Note: macOS requires Location Services to be enabled for Kaspersky VPN to obtain a Wi-Fi network name (BSSID). Kaspersky Security Network will use this to detect unsecured Wi-Fi networks. It won't be used to determine your real location.

3. Follow the instructions on the screen.

The application will use Kaspersky Security Network to detect unsecured Wi-Fi networks.

Select the action Kaspersky VPN performs when you join an unsecured Wi-Fi network

You can select whether you want Kaspersky VPN to prompt you for action or secure the connection automatically when you join an unsecured Wi-Fi network.

[Select the action Kaspersky VPN performs when you join an unsecured Wi-Fi network](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. On the **Unsecured Wi-Fi** tab, select the action you want Kaspersky VPN to perform.

How to get customer service

If you cannot find a solution to your issue in the documentation or in [any of the sources of information about the application](#), we recommend that you contact Customer Service. Visit the [Customer Service website](#) to contact our experts, who can answer all your questions about installing and using the application.

Note: Before contacting Customer Service, please read the [support rules](#).

Known issues

While using Kaspersky VPN, you may encounter the following known issues:

- If Power Nap is enabled on your Mac, Kaspersky VPN does not protect all information updates as the program does not run while your Mac is sleeping. If you need to protect all your data sent and received through the internet, we recommend that you disable Power Nap on your Mac.
- If Kaspersky Security Cloud / Kaspersky Internet Security for Mac is installed on your Mac and Kill Switch is turned on, then Kaspersky VPN can't establish an encrypted secure connection. To establish a secure connection, turn off Kill Switch or quit Kaspersky Security Cloud / Kaspersky Internet Security for Mac. This is due to certain macOS issues. We've contacted Apple regarding this issue and are doing our best to fix the problem as soon as possible.
- An encrypted secure connection cannot be established from the macOS system settings.
- The volume of used secure traffic displayed in the application may differ from the amount of secure traffic actually used. This may be the case when you use a high-bandwidth connection.
- When the application changes the virtual server, the secure connection may be briefly interrupted. Transmitted data will not be protected until the secure connection has been reestablished.
- After purchasing a subscription, there may be a delay of several minutes before the application switches to the Unlimited version.
- If your Mac changes the network when connecting to the internet, the secure connection may be briefly interrupted. Transmitted data will not be protected until the secure connection has been reestablished.
- Changing the virtual server when visiting the websites of banks or payment systems, booking websites, social networks, chats, and email websites could possibly trigger anti-fraud systems (systems intended for analyzing online financial transactions for signs of fraudulent operations).
- When your Mac changes its power source (battery/plugged in), the secure connection may be briefly interrupted. The transmitted data is not protected until the secure connection is reestablished. The Kill Switch doesn't cut off data transfer in this case. This is due to certain macOS issues. We've contacted Apple regarding this issue and are doing our best to fix the problem as soon as possible.
- If you sign out from your My Kaspersky account while connected through a VPN and you have an active subscription, the secure connection may be interrupted. Transmitted data will not be protected until you reestablish the secure connection.
- iCloud Private Relay and Mail Privacy Protection are incompatible with Kaspersky VPN on macOS 12 or later.

You may experience problems when connecting to certain websites through a VPN.

Some websites and web services deny access when you try to connect to them through a VPN. Websites and web services may deny VPN access for the following reasons:

- Website owners want the licensed content they publish to only be available for a certain country, since there are different offers and prices for different countries.
- Website owners want the website to only be visited from a certain region. For example, a lottery is drawn only for a certain country, so access from other regions is forbidden.
- There are web services that, for legal reasons, are only available in a particular region (for example, some media services providers or news broadcasters). These web services resist anonymizers and are not available when you use a VPN (or another anonymizer) to reach them.

- These web services not only determine the location of the client, but also determine if the client uses an anonymizer. If an attempt to access the web service via an anonymizer is detected, access to the web service is blocked.
- If you cannot access a certain website or web service by using a Kaspersky VPN, we recommend [contacting Customer Service](#). Report the web service that is unavailable and from which location. Kaspersky will do our best to resolve the issue.
- Your internet connection speed may be reduced by more than 50 percent with Kaspersky VPN running. We cannot guarantee a minimum internet connection speed.
- Kaspersky VPN can't establish an encrypted secure connection for web traffic sent and received via the IPv6 protocol. IPv6 web traffic is blocked while VPN is active. On devices that only support the IPv6 protocol, Kaspersky VPN can't establish an encrypted connection and protect your web traffic.
- If an IPv6 connection was established before VPN was turned on, IPv6 web traffic will briefly not be blocked.

Sources of information about the application

Kaspersky VPN page on the Kaspersky website

On the [Kaspersky VPN page on the Kaspersky website](#), you can view general information about the application, its functions, and features.

Kaspersky VPN page in the Knowledge Base

The *Knowledge Base* is a section on the Kaspersky Customer Service website.

On the [Kaspersky VPN page in the Knowledge Base](#), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to buy, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky VPN as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Customer Service news.

[Go to the Knowledge Base from the Help pull-down menu](#)

Choose **Help** > **Support**.

Discuss Kaspersky applications on Kaspersky Support Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on [our Forum](#).

On the Forum, you can view discussion topics, post your comments, and create new discussion topics.

[Go to the Forum from the Help pull-down menu](#)

Choose **Help** > **Community**.

Note: An internet connection is required to access website resources.

If you can't find a solution to your problem, [contact Customer Service](#).

Legal

View the terms and conditions of the End User License Agreement and the Marketing Statement

You can review the terms of the License Agreement using the following methods:

- On the App Store
- By reading the license.txt file in the folder where the application has been installed

[Read the Marketing Statement and disable sending data](#)

1. In the menu bar, click the application icon and choose **Preferences**.

The application settings window opens.

2. In the **Improved experience** section, click **Show Marketing Statement** if you want to read the terms of the Marketing Statement.

A window with the Marketing Statement opens.

3. If you want to disable sending data, deselect the **Help Kaspersky improve its products by sending information about the application and its operating environment** checkbox.

Information about third-party code

Information about third-party code is contained in the legal_notices.txt file in the folder where the application has been installed.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

App Store, Apple, Finder, iCloud, iTunes, Launchpad, Mac, macOS, OS X and Touch ID are trademarks of Apple Inc., registered in the U.S. and other countries and regions.

IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Android, Firebase, Google, and Google Play are trademarks of Google LLC.

Microsoft and Windows are trademarks of the Microsoft group of companies.

JavaScript is a registered trademark of Oracle and/or its affiliates.

Intel is a trademark of Intel Corporation in the U.S. and/or other countries.

The "Create a My Kaspersky account" window

Enter email address field

Email address that you want to use with your new My Kaspersky account.

This email address is used to recover your password and receive communications from Kaspersky.

Choose password field

Password for your new My Kaspersky account. The password must contain a minimum of eight characters, including at least one digit, one lowercase letter, and one uppercase letter. Spaces are not allowed.

Confirm password field

Confirmation of the password for your new My Kaspersky account.

By default, the password characters are hidden for security reasons. To view the password, click the eye icon .

Country selection pop-up menu

A pop-up menu from which you can choose the country for My Kaspersky. This option determines the regional settings for your My Kaspersky account, for example, the display language and available Kaspersky applications. You can change your region for My Kaspersky later only by contacting Customer Service.

I confirm that I have fully read, understand, and accept the terms and conditions of the Privacy Policy describing the handling of data

If this checkbox is selected, it means that you agree with the terms of the Privacy Policy, which describes how data is handled.

Note: The **Create** button becomes available only if you confirm that you have fully read, understand, and accept the Privacy Policy.

I agree to provide Kaspersky with my email address to receive personalized marketing offers

This checkbox enables/disables delivery of email messages with information and promotions from Kaspersky to the specified email address.

Create

Clicking this button creates your new My Kaspersky account.

The "Sign In to My Kaspersky" window

Sign in with Google

Clicking this button opens a browser window where you can sign in to My Kaspersky with your Google account.

Sign in with Facebook

Clicking this button opens a browser window where you can sign in to My Kaspersky with your Facebook account.

Note: The availability of the option to sign in with Facebook depends on your region.

Sign in with Apple

Clicking this button opens a system window where you can sign in to My Kaspersky with your Apple ID.

Email address field

Email address associated with your My Kaspersky account.

Password field

Password for your My Kaspersky account.

By default, the password characters are hidden for security reasons. To view the password, click the eye icon .

Forgot your password?

Clicking this link opens a browser window where you can reset the password for your My Kaspersky account.

Sign In

Clicking this button connects Kaspersky VPN to My Kaspersky.

Create Account

Clicking this button opens a window where you can create a My Kaspersky account.

The "General" tab

In the **Run in background** section, you can configure whether Kaspersky VPN will run in the background and establish a secure connection right after your Mac starts.

Let Kaspersky VPN run in the background (recommended)

This checkbox enables/disables running Kaspersky VPN in the background.

Turn on VPN automatically when your Mac starts

This checkbox enables/disables establishing a secure connection right after your Mac starts.

This checkbox is available if the **Let Kaspersky VPN run in the background (recommended)** checkbox is selected.

In the **Improved experience** section, you can read the terms of the Marketing Statement and agree or disagree to send the information listed in the Marketing Statement to Kaspersky.

Help Kaspersky improve its products by sending information about the application and its operating environment

This checkbox enables/disables sending information listed in the Marketing Statement to Kaspersky.

Show Marketing Statement

Clicking this link opens a window that displays the text of the Marketing Statement.

The "Split Tunneling" tab

On the **Split Tunneling** tab, you can configure enabling a VPN connection only for selected applications.

Note: Split Tunneling is available only in the Unlimited version of Kaspersky VPN.

Turn on VPN only for selected apps

This checkbox enables/disables Split Tunneling. When Split Tunneling is enabled, only selected applications from the list below will connect via a VPN while other apps will connect directly to the internet.

This checkbox is unselected by default.

The "Kill Switch" tab

On the **Kill Switch** tab, you can configure whether your data will be protected when the VPN connection is interrupted.

Note: Kill Switch is available only in the Unlimited version of Kaspersky VPN.

Turn on Kill Switch

This checkbox enables/disables Kill Switch. Kill Switch cuts off data transfer over the internet when VPN is reconnecting. Your internet connection will be restored as soon as VPN turns on.

This checkbox is unselected by default.

The "Unsecured Wi-Fi" tab

On the **Unsecured Wi-Fi** tab, you can select an action that Kaspersky VPN performs when you join an unsecured Wi-Fi network.

Detect unsecured Wi-Fi networks

This checkbox enables/disables detection of unsecured Wi-Fi networks.

Enable cloud detection with Kaspersky Security Network

This checkbox enables/disables detection of unsecured Wi-Fi networks with Kaspersky Security Network. When you select this checkbox for the first time, you need to enable Location Services for Kaspersky VPN.

Note: macOS requires Location Services to be enabled for Kaspersky VPN to obtain a Wi-Fi network name (BSSID). Kaspersky Security Network will use this to detect unsecured Wi-Fi networks. It won't be used to determine your real location

Prompt for action

Kaspersky VPN prompts you to choose an action when you join an unsecured Wi-Fi network.

This action is selected by default.

Turn on VPN automatically

Kaspersky VPN automatically turns on VPN when you join an unsecured Wi-Fi network.

Network Name

This column displays the name of the Wi-Fi network.

Last Connected

This column displays the date of the last connection to the Wi-Fi network.

Upon Connecting to Wi-Fi Network

This column displays the action Kaspersky VPN performs upon connecting to the Wi-Fi network:

Not Specified

If the specified Wi-Fi network is unsecured, the application applies the settings specified for unsecured Wi-Fi networks. If the specified network is secure, the application does nothing.

Turn VPN On

The application turns on VPN when you connect your Mac to the specified Wi-Fi network.

No Action

The application does not turn on VPN when you connect your Mac to the specified Wi-Fi network.

The "Your account is almost ready" window

Region selection pop-up menu

A pop-up menu from which you can choose the region for My Kaspersky. This option determines the regional settings for your My Kaspersky account, for example, the display language and available Kaspersky applications. You can change your region for My Kaspersky later only by contacting Customer Service.

I confirm that I have fully read, understand, and accept the terms and conditions of the Privacy Policy describing the handling of data

If this checkbox is selected, it means that you agree with the terms of the Privacy Policy, which describes how data is handled.

I agree to provide Kaspersky with my email address to receive personalized marketing offers

This checkbox enables/disables delivery of email messages with information and promotions from Kaspersky to the specified email address.

Create

Clicking this button creates your new My Kaspersky account.

The "Proxy server authentication required" dialog

User Name:

Field for entering the user name for connecting to the proxy server.

Password:

Field for entering the password.

Remember password

This checkbox enables/disables the use of the specified user name and password for authentication on the proxy server in the future.

This checkbox is unselected by default.