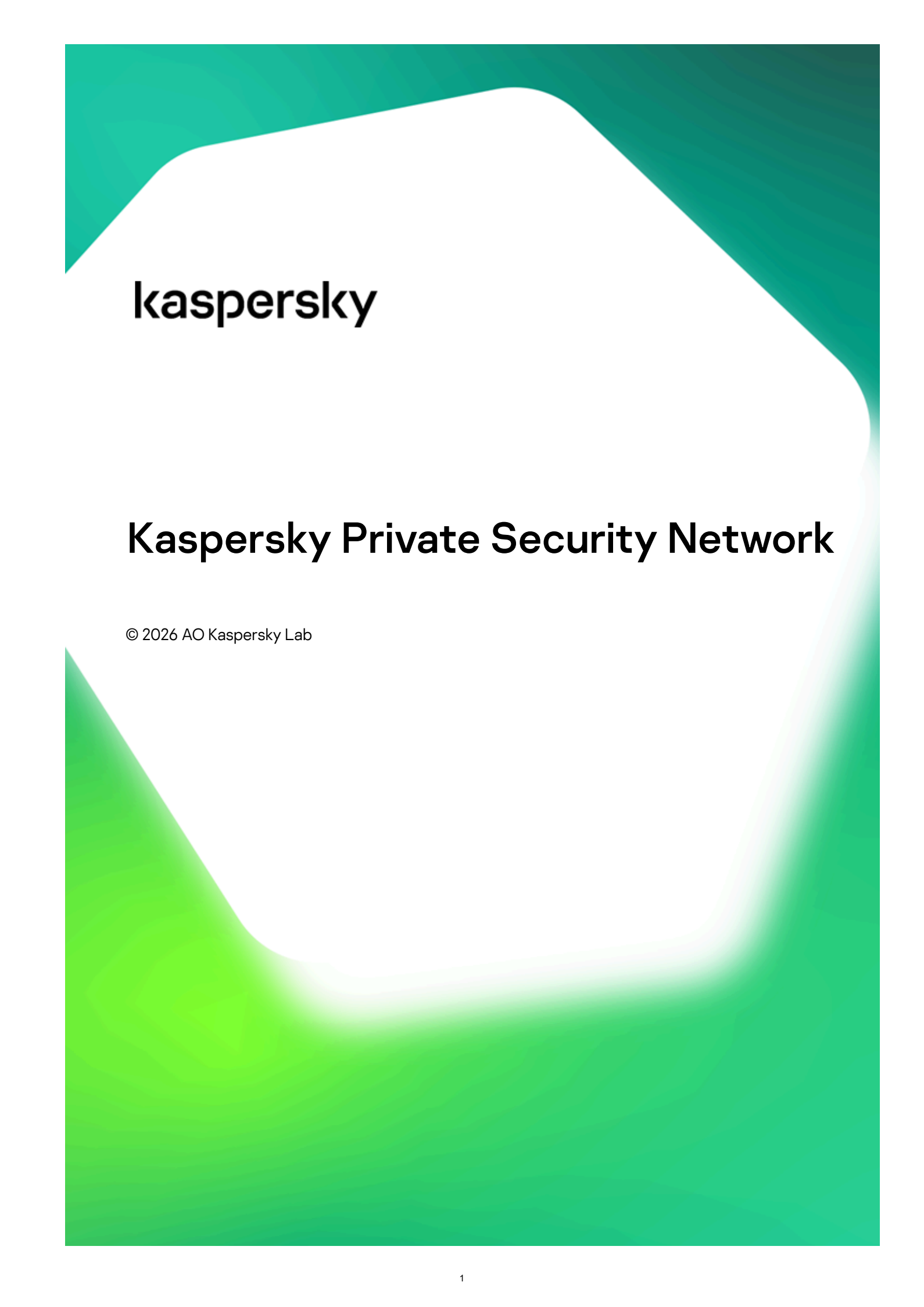


The background of the entire page is a vibrant green with a subtle gradient. A large, white, rounded rectangular shape is centered on the page, creating a frame for the text. The Kaspersky logo is positioned in the upper left of this white area.

kaspersky

Kaspersky Private Security Network

© 2026 AO Kaspersky Lab

Contents

[About Kaspersky Private Security Network](#)

[About Kaspersky Security Network](#)

[How Kaspersky Private Security Network differs from Kaspersky Security Network](#)

[What's new in Version 4.0](#)

[Distribution kit](#)

[Kaspersky Private Security Network licensing](#)

[Hardware and software requirements](#)

[Application architecture](#)

[Common deployment scenarios](#)

[Simplified deployment scenarios](#)

[Deploying Kaspersky Private Security Network with redundancy](#)

[Managing access permissions](#)

[Adding or removing a server](#)

[Installing Kaspersky Private Security Network](#)

[Preparing to install Kaspersky Private Security Network](#)

[Installing the server part of Kaspersky Private Security Network](#)

[Preparing an integration file for the Kaspersky Private Security Network web plug-in](#)

[Installing the Kaspersky Private Security Network web plug-in](#)

[Step 1. Integration of the server part of Kaspersky Private Security Network and the Kaspersky Private Security Network web plug-in](#)

[Step 2. Uploading the activation archive](#)

[Step 3. Selecting components for installation](#)

[Step 4. Installing components](#)

[Step 5. Adding traffic encryption keys](#)

[Step 6. Adding an installation ID](#)

[Step 7. Checking the configuration](#)

[Finishing the installation](#)

[Updating Kaspersky Private Security Network](#)

[Updating the Kaspersky Private Security Network web plug-in](#)

[Updating the server part of Kaspersky Private Security Network](#)

[Updating Kaspersky Private Security Network to version 4.0.1](#)

[Updating Kaspersky Private Security Network to version 4.0.2](#)

[Updating Kaspersky Private Security Network to version 4.0.3](#)

[Updating Kaspersky Private Security Network to version 4.0.4](#)

[Updating Kaspersky Private Security Network to version 4.0.5](#)

[Updating Kaspersky Private Security Network to version 4.0.6](#)

[Removing the integration with Kaspersky Private Security Network](#)

[Removing Kaspersky Private Security Network](#)

[Certificate for receiving updates](#)

[Database update](#)

[Database update request](#)

[Monitoring database updates](#)

[Troubleshooting problems with data transfer via a unidirectional gateway](#)

[Configuring a proxy server](#)

[Kaspersky Private Security Network configuration](#)

[Viewing information about the configuration](#)

[Adding and removing components](#)

[Getting Kaspersky Private Security Network configuration files](#)

[Encrypting traffic](#)

[Creating a traffic encryption key](#)

[Adding a traffic encryption key](#)

[Exporting and importing the traffic encryption key store](#)

[Kaspersky Private Security Network service access addresses](#)

[Managing local reputation databases](#)

[Adding and updating file or URL reputation data](#)

[Exporting the local reputation database to a text file](#)

[Deleting file or URL reputation records](#)

[Monitoring the operation of Kaspersky Private Security Network](#)

[Monitoring the status of components and servers](#)

[Monitoring the reputation of objects](#)

[Monitoring the request processing time](#)

[Monitoring the database lag](#)

[Troubleshooting Kaspersky Private Security Network components](#)

[Notifications about Kaspersky Private Security Network events](#)

[Configuring email notifications about Kaspersky Private Security Network events](#)

[Configuring the logging of Kaspersky Private Security Network events in Syslog](#)

[KPSN API](#)

[Getting started with the API](#)

[Making API requests](#)

[Adding file reputation data](#)

[Adding URL reputation data](#)

[Deleting file reputation data](#)

[Deleting URL reputation data](#)

[Verifying the reputation of files](#)

[Verifying the reputation of websites](#)

[Error codes](#)

[Kaspersky Private Security Network log](#)

[Enabling or disabling request logging for URL Reputation and File Reputation services](#)

[Contacting the Technical Support Service](#)

[How to get technical support](#)

[Technical support via Kaspersky CompanyAccount](#)

[Appendix](#)

[List of ports used by Kaspersky Private Security Network](#)

[List of website categories of the URL Reputation service](#)

[Updating third-party software used by Kaspersky Private Security Network 4.0.3 or higher](#)

[Updating third party software](#)

[Updating third-party software in configuration with a unidirectional gateway](#)

[Rolling back third-party software to versions used by Kaspersky Private Security Network by default](#)

[Sources of information about the application](#)

Glossary

[Anti-Spam](#)

[Categorized network segment](#)

[Cloud Information](#)

[File Reputation](#)

[Gateway External](#)

[Gateway Internal](#)

[Kaspersky categories](#)

[Kaspersky Security Network \(KSN\)](#)

[MD5](#)

[Open network segment](#)

[Record Management](#)

[Spam](#)

[SSL](#)

[Traffic encryption key](#)

[Unidirectional gateway](#)

[URL Reputation](#)

[Information about third-party code](#)

[Trademark notices](#)

About Kaspersky Private Security Network

Kaspersky Private Security Network is a solution that gives users of computers with Kaspersky applications installed ("the company's computers") access to reputation databases of [Kaspersky Security Network](#) and other statistical data without sending data from their computers to Kaspersky Security Network.

The Kaspersky Private Security Network solution (hereinafter also referred to as *KPSM*) is designed for corporate customers that are unable to participate in Kaspersky Security Network for any of the following reasons:

- Local workstations are not connected to the Internet
- Transmission of any data out of the country or the corporate LAN is prohibited by corporate security policies or applicable law

The updates functionality (including antivirus signature updates and codebase updates), and KSN functionality may not be available in the application in the United States.

Kaspersky Private Security Network can be used with the following Kaspersky applications:

- Kaspersky Anti Targeted Attack Platform.
- Kaspersky Security Center.
- Kaspersky Endpoint Detection and Response.
- Kaspersky Secure Mail Gateway.
- Kaspersky Web Filter Software Development Kit.
- Kaspersky Web Traffic Security.
- Starting with Kaspersky Private Security Network 4.0.5: Kaspersky Anti-Virus Software Development Kit Level 3 for Windows® version 8.10.2 and later.
- Starting with Kaspersky Private Security Network 4.0.6: Kaspersky Anti-Virus Software Development Kit Level 3 for Linux® version 8.10.4 and later.
- Starting with Kaspersky Private Security Network 4.0.6: Kaspersky Anti-Virus Software Development Kit Level 3 for Mac® version 8.10.4 and later.

Kaspersky Private Security Network together with Kaspersky Security Center can be used with the following Kaspersky applications:

- Kaspersky Embedded Systems Security.
- Kaspersky Endpoint Security for Android™.
- Kaspersky Endpoint Security for Linux.
- Kaspersky Endpoint Security for Mac.
- Kaspersky Endpoint Security for Windows.

- Kaspersky Industrial Cyber Security for Nodes.
- Kaspersky Security for Windows Server®.
- Kaspersky Security for Virtualization Agentless.
- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Security for Storages.

For details on using Kaspersky Private Security Network with Kaspersky applications, please refer to the documentation of the relevant applications.

You can use Kaspersky Private Security Network in the following configurations:

- **Standard**

This option is used if all servers hosting Kaspersky Private Security Network components are allowed access to Kaspersky servers to receive reputation database packages.

- **With a proxy server**

This option is used if access to Kaspersky servers is blocked on the corporate LAN. In this case, the corporate LAN is divided into an [open](#) network segment and a [categorized](#) network segment. Interaction with Kaspersky servers is conducted via the proxy server of your organization's network.

- **With a unidirectional gateway**

This option is used if access to Kaspersky servers is blocked on the corporate LAN. In this case, the corporate LAN is divided into an open network segment and a categorized network segment. A [unidirectional gateway](#) is used for interaction between the network segments.

The configuration of Kaspersky Private Security Network is determined by the corporate security requirements.

About Kaspersky Security Network

Kaspersky Security Network is an infrastructure of cloud services providing access to Kaspersky's online knowledge base with the following information:

- Reputation of files, websites, and applications
- [Categories](#) of files, websites, and applications (e.g., an operating system file, computer game, adult content website)
- Frequency of file detection in all countries of the world and geography of file distribution
- Statistics on how files and websites are trusted by users of Kaspersky applications worldwide
- Recalls by Kaspersky virus analysts of individual virus signatures in local databases of anti-virus applications (e.g. changing reputation of an object from "dangerous" to "safe")

Kaspersky Security Network data is used in Kaspersky applications for the following purposes:

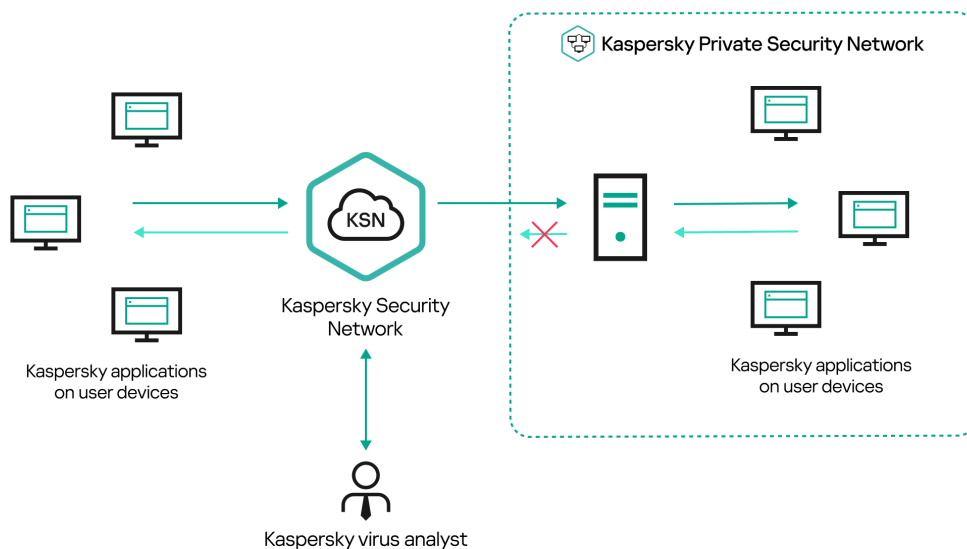
- Provide up-to-date information about objects that are not yet reflected in malware databases
- Reduce the probability of Anti-Spam false alarms
- Block user access to malicious websites
- Block execution of malicious files on the user's computer
- Restrict access to specific categories of files and websites (e.g., restrict files and websites of the Computer Games category from being opened during office hours)

If the user participates in Kaspersky Security Network, the Kaspersky application installed on the user's computer receives information from Kaspersky Security Network and sends to Kaspersky information about potentially dangerous objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in reputation and statistical databases of Kaspersky Security Network.

How Kaspersky Private Security Network differs from Kaspersky Security Network

Unlike with Kaspersky Security Network, users of Kaspersky Private Security Network are able to receive information from the Kaspersky knowledge base without sending data to Kaspersky Security Network from their computers.

Differences between the operating principles of Kaspersky Security Network and Kaspersky Private Security Network are shown in the figure below.



Comparison of operating principles of Kaspersky Security Network and Kaspersky Private Security Network

What's new in Version 4.0

Kaspersky Private Security Network 4.0

Kaspersky Private Security Network 4.0 introduces the following features and improvements:

- The user interface of Kaspersky Private Security Network is updated: Kaspersky Private Security Network is now a web plug-in within the web interface of Kaspersky Security Center Web Console.
- The Kaspersky Private Security Network Setup Wizard has been added.
- Added support for using the organization's proxy server.
- You can use the web interface to get files with settings for connecting to servers of the Kaspersky Private Security Network service.
- Updates of the file reputation database for the File Reputation service contain records that identify files by both its MD5 hash and SHA256 hash.

Kaspersky Private Security Network 4.0.1

Kaspersky Private Security Network 4.0.1 introduces the following features and improvements:

- The selection of the time interval displayed in charts is improved.
- For the Gateway Internal and Gateway External components, the interface now displays the server on which the component is installed.

Kaspersky Private Security Network 4.0.2

Kaspersky Private Security Network version 4.0.2 fixes errors found in versions 4.0 and 4.0.1.

Kaspersky Private Security Network 4.0.3

Kaspersky Private Security Network 4.0.3 introduces the following features and improvements:

- Newer versions of third-party code used by the application.
- Now you can [update the versions of containers of third-party software used by the application.](#)

Kaspersky Private Security Network 4.0.4

Kaspersky Private Security Network 4.0.4 introduces the following features and improvements:

- Added support for new versions of the K3s orchestrator.
- Added support for Red Hat Enterprise Linux 9.6.

Kaspersky Private Security Network 4.0.5

Kaspersky Private Security Network 4.0.5 introduces the following features and improvements:

- Compatibility with new versions of third-party software.
- Compatibility with KAV SDK L3 for Windows version 8.10.3 or later.

Kaspersky Private Security Network 4.0.6

Kaspersky Private Security Network 4.0.6 introduces the following features and improvements:

- Compatibility with new versions of third-party software.
- Improved component monitoring.

Distribution kit

The Kaspersky Private Security Network distribution kit includes the following components:

- Installation archive of the Kaspersky Private Security Network web plug-in for Kaspersky Security Center
- Installation archive of the server part of Kaspersky Private Security Network
- Release Notes of Kaspersky Private Security Network

Kaspersky Private Security Network licensing

About the End User License Agreement

The *End User License Agreement* is a legal agreement between you and AO Kaspersky Lab, which specifies the terms and conditions on which you can use Kaspersky Private Security Network.

Thoroughly read the terms and conditions of the End User License Agreement before you start using the Kaspersky Private Security Network.

You can read the End User License Agreement in any of the following ways:

- When installing the server part of Kaspersky Private Security Network.
- On the server where the server part of Kaspersky Private Security Network is installed, using the `kpsnctl show-eula` command

You can find the `kpsnctl` utility in the installation archive of the server part of Kaspersky Private Security Network.

You accept the terms of the End User License Agreement by confirming your consent to the text of the End User License Agreement when you install the server part of KPSN, namely by specifying the `--accept-eula` option when starting the installation. If you do not accept the terms and conditions of the End User License Agreement, you may not use Kaspersky Private Security Network.

About the license

A *license* is a time-limited right to use Kaspersky Private Security Network, granted under the End User License Agreement.

The license term is equal to the validity period of the [update certificate](#).

A license entitles you to the following kinds of services:

- Use of the web plug-in and the server part of Kaspersky Private Security Network
- Assistance from Kaspersky Technical Support
- Other services available from Kaspersky or its partners during the term of the license

The functionality of Kaspersky Private Security Network available under the license depends on the type of license. The Kaspersky Private Security Network license can have the following types:

- **Kaspersky Private Security Network Standard**

Support of up to 50 thousand devices.

- **Kaspersky Private Security Network Advanced**

- Support of up to 500 thousand devices.
- Managing the local reputation databases (corporate allow and deny lists of files and addresses).
- Support of the service provider model (xSP model).
- High availability (up to 10 nodes with clustering capability).

About the License Certificate

The *License Certificate* is a document that is handed over to you with the distribution kit.

The License Certificate contains the following information about the license being provided:

- Order number
- Information about the user to which the license is provided
- Information about the application that can be activated using the provided license
- Limitation of the number of licensing units (for example, devices on which the application can be used under the provided license)
- Start date of the license term
- End date or duration of the license term
- Type of the license

Hardware and software requirements

Software requirements for installing the server part of Kaspersky Private Security Network

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Kaspersky Private Security Network 4.0-4.0.3

Each server where you intend to install Kaspersky Private Security Network components must have the following software:

- Ubuntu 24.04 LTS operating system.
- Helm® 3.x.x, version 3.15.3 or later.
- K3s orchestrator of the following versions:
 - 1.29.1–1.29.15.
 - 1.30.0–1.30.14.
 - 1.31.0–1.31.5.
 - 1.32.0–1.32.1.

The traefik component must be disabled in K3s orchestrator.

The servers must be combined into a Kubernetes® cluster managed by the K3s orchestrator.

Kaspersky Private Security Network uses the entire cluster.

Kubernetes can be used to add servers to the cluster after Kaspersky Private Security Network is installed.

Kaspersky Private Security Network 4.0.4

Each server where you intend to install Kaspersky Private Security Network components must have the following software:

- Operating system: Ubuntu 24.04 LTS or Red Hat Enterprise Linux 9.6.
- Helm® 3.x.x, version 3.15.3 or later.
- K3s orchestrator of the following versions:
 - 1.29.1–1.29.15.
 - 1.30.0–1.30.14.
 - 1.31.0–1.31.13.
 - 1.32.0–1.32.9.
 - 1.33.0–1.33.5.
 - 1.34.1.

The traefik component must be disabled in the K3s orchestrator.

The servers must be combined into a Kubernetes® cluster managed by the K3s orchestrator.

Kaspersky Private Security Network uses the entire cluster.

Kubernetes can be used to add servers to the cluster after Kaspersky Private Security Network is installed.

Kaspersky Private Security Network 4.0.5

Each server where you intend to install Kaspersky Private Security Network components must have the following software:

- Operating system: Ubuntu 24.04 LTS or Red Hat Enterprise Linux 9.6.
- Helm® 3.19.0 or later.
- K3s orchestrator of the following versions:
 - 1.32.2–1.32.13
 - 1.33.0–1.33.9
 - 1.34.1–1.34.5
 - 1.35.0–1.35.2

The traefik component must be disabled in the K3s orchestrator.

The servers must be combined into a Kubernetes® cluster managed by the K3s orchestrator.

Kaspersky Private Security Network uses the entire cluster.

Kubernetes can be used to add servers to the cluster after Kaspersky Private Security Network is installed.

Kaspersky Private Security Network 4.0.6

Each server where you intend to install Kaspersky Private Security Network components must have the following software:

- Operating system: Ubuntu 24.04 LTS, Red Hat Enterprise Linux 9.8.
- Helm® 4.1.1 and K3s orchestrator 1.35.2, or Helm 4.3.0 and K3s orchestrator 1.36.4.

The traefik component must be disabled in the K3s orchestrator.

The servers must be combined into a Kubernetes® cluster managed by the K3s orchestrator.

Kaspersky Private Security Network uses the entire cluster.

Kubernetes can be used to add servers to the cluster after Kaspersky Private Security Network is installed.

Hardware requirements for installing the server part of Kaspersky Private Security Network

Hardware requirements for the servers included in the cluster are listed in the tables below. Kaspersky Private Security Network components are automatically distributed among the servers within the cluster. The components are installed according [to the deployment scenario](#).

Deployment scenario	Installed components	Hardware requirements
Standard	- File Reputation. - URL Reputation - Anti-Spam. - Cloud Information. - Certificate Validation. - RMS.	- CPU: 2.8 GHz, 16 cores. - RAM size: 116 GB. - Disk subsystem: 1 TB SSD (at least 50,000 read/write operations per second). - Additional free space is required for working with the local reputation database of the File Reputation service. 2 GB of disk space is required for every 1 million records. - Additional free space is required for working with the local reputation database of the URL Reputation service. 2 GB of disk space and 0.5 GB of RAM is required for every 1 million records.
With a unidirectional gateway	Cluster in the open segment: Gateway External	- CPU: 2 GHz, 4 cores. - RAM size: 16 GB. - Disk subsystem: 72 GB of free space.
	Cluster in the categorized segment: - Gateway Internal - File Reputation. - URL Reputation - Anti-Spam. - Cloud Information. - Certificate Validation. - RMS.	- CPU: 2.8 GHz, 16 cores. - RAM size: 116 GB. - Disk subsystem: 1.5 TB SSD (at least 50,000 read/write operations per second). - Additional free space is required for working with the local reputation database of the UrlReputation service. 1 GB of disk space and 0.5 GB of RAM is required for every 1 million records.
	Unidirectional gateway	Not provided.

Network requirements: network interface with a bandwidth of 100 Mbit/sec.

Confidential information (such as application logs) is stored on Kaspersky Private Security Network servers. You are advised to provide additional security for Kaspersky Private Security Network servers. After configuring additional security measures, make sure that the connections required by the application are available.

Software requirements for installing the web plug-in

The plug-in must be installed on a server with Kaspersky Security Center Kaspersky Security Center Web Console installed. Supported versions of Kaspersky Security Center:

- Kaspersky Security Center 14.2 Windows
- Kaspersky Security Center 15.1 Windows
- Kaspersky Security Center 15 Linux
- Kaspersky Security Center 15.1 Linux
- Kaspersky Security Center 15.2 Linux
- Kaspersky Security Center 15.3 Linux
- Kaspersky Security Center 15.4 Linux
- Kaspersky Security Center 16 Linux
- Kaspersky Security Center 16.1 Linux

- Kaspersky Security Center 16.2 Linux
- Kaspersky Security Center 16.3 Linux
- Kaspersky Security Center 17 Linux

A browser must be installed on the computer that will be used for managing the Kaspersky Private Security Network web plug-in. There are no restrictions on the types and versions of browsers used for this purpose. Google™ Chrome™, Mozilla™ Firefox™, or Microsoft® Edge browsers are recommended.

Hardware requirements for installing the web plug-in

The hardware requirements for the Kaspersky Security Center server, on which you will install the Kaspersky Private Security Network web plug-in are the same as the hardware requirements of Kaspersky Security Center. For more details, please refer to the *Kaspersky Security Center Help*.

Application architecture

The functionality of Kaspersky Private Security Network is provided by two principal components:

- The Kaspersky Private Security Network web plug-in provides a web interface for managing Kaspersky Private Security Network. The web plug-in communicates with the server part of Kaspersky Private Security Network over an encrypted link.

The Kaspersky Private Security Network web plug-in is [installed manually](#) in the Kaspersky Security Center Web Console.

A [supported browser](#) must be installed on computers from which Kaspersky Private Security Network is managed through the web plug-in in Kaspersky Security Center Web Console. These computers must also have access to the servers on which the Kaspersky Security Center Web Console application is installed.

- The server part of Kaspersky Private Security Network, which includes the following components:

- **Gateway External**

The Gateway External component keeps the reputation databases of Kaspersky Private Security Network components updated in a configuration with a unidirectional gateway.

The Gateway External component performs the following functions:

- Gets reputation database packages for Kaspersky Private Security Network components from Kaspersky servers.
- Verifies the integrity of received data.
- Creates and sends reputation database packages through a unidirectional gateway to the categorized network segment, to the server hosting the Gateway Internal component.

The Gateway External component is installed in the open network segment.

- **Gateway Internal**

The Gateway Internal component keeps the reputation databases of Kaspersky Private Security Network components updated in a configuration with a unidirectional gateway.

The Gateway Internal component performs the following functions:

- Gets reputation database packages through the unidirectional gateway from the server hosting the Gateway External component located in the open network segment.
- Verifies the integrity of received data.
- Updates the reputation databases of Kaspersky Private Security Network components on servers of the categorized network segment.

The Gateway Internal component is installed on a server in the categorized network segment.

- **Cloud Information**

The Cloud Information component provides Kaspersky applications with information about the general indicators of object reputation databases.

Based on information from this component, Kaspersky applications can display, for example, the number of objects with a certain reputation (dangerous, safe, and other).

- **File Reputation**

The File Reputation component provides the following information to Kaspersky applications:

- File reputation
- File category (for example, operating system file)
- Detection frequency for file in all countries of the world and the geographic extent of the file's spread

Kaspersky applications can use this information to detect malicious files on computers of users. After detecting a malicious file, the application performs the action specified in the application settings: disinfection, deletion, or blocking. Based on information from this component, Kaspersky applications can also restrict the startup of individual categories of files, such as files in the Computer Games category.

- **URL Reputation**

The URL Reputation component provides Kaspersky applications with information on the reputation of websites and the website category (e.g., adult content).

Kaspersky applications can use information from this component to block access to malicious websites on computers of users and restrict access to certain categories of websites.

- **Certificate Validation**

The Certificate Validation component provides Kaspersky applications with file reputation information based on the reputation of the certificates that they are signed with. If a file is signed with a certificate from a trusted source, the file is also trusted. For example, an application is considered trusted if it is signed with a certificate provided by the official store.

Based on this information, Kaspersky applications can determine the reputation of files that are signed with certificates (trusted or untrusted).

- **Anti-Spam**

The Anti-Spam component provides statistical data to Kaspersky mail server protection applications that lets them protect the mail traffic and filter out unwanted messages (spam). For more details on the operation of mail server protection applications, please refer to the [documentation on these applications](#) ².

- **Record Management System (RMS)**

The RMS component supplies information about the reputation of objects to Kaspersky anti-virus applications. The information is provided by Kaspersky virus analysts.

This component is used to quickly process changes of object reputation from "trusted" to "untrusted". The RMS component monitors information about the reputation of objects and, in case of changes, updates information about the relevant object in the anti-virus databases used by Kaspersky applications.

The server part of Kaspersky Private Security Network is deployed in a Kubernetes cluster on the corporate network. The servers must satisfy the [hardware and software requirements](#). The architecture of Kaspersky Private Security Network and the presence or absence of server-side components depend on the [configuration of the application](#).

You can select the server components that you want to install when [installing the Kaspersky Private Security Network web plug-in in the Kaspersky Security Center Web Console](#). You can view information about the installed components of Kaspersky Private Security Network [in the web interface of Kaspersky Security Center Web Console](#).

To ensure the security of data transfer between the Kaspersky Private Security Network and applications on the corporate LAN, you must [add a traffic encryption key](#).

Interaction between the Kaspersky Private Security Network and Kaspersky Security Network is carried out over an encrypted channel using a client certificate for authorization, which is issued separately.

The kpsnctl utility allows the administrator to manage the integration of the server part of Kaspersky Private Security Network with the web plug-in, the root certificate in the Kaspersky Private Security Network certificate hierarchy, and the server certificate. The administrator can also use the kpsnctl utility to view the [Kaspersky Private Security Network End User License Agreement](#).

Common deployment scenarios

This section describes the common Kaspersky Private Security Network deployment scenarios.

The Kaspersky Private Security Network deployment scenario depends on the number of Kaspersky applications used by your company, the expected load on Kaspersky Private Security Network servers, and the corporate security requirements.

Simplified deployment scenarios

Simplified deployment scenarios involve the deployment of Kaspersky Private Security Network components as a single instance.

Kaspersky Private Security Network can be deployed in the following configurations:

- Standard
- With a proxy server
- With a unidirectional gateway

The choice of configuration for Kaspersky Private Security Network is determined by the corporate security requirements of your organization.

Standard configuration of Kaspersky Private Security Network

The standard configuration of Kaspersky Private Security Network is used if all servers on which the Kaspersky Private Security Network components are installed have access to Kaspersky servers.

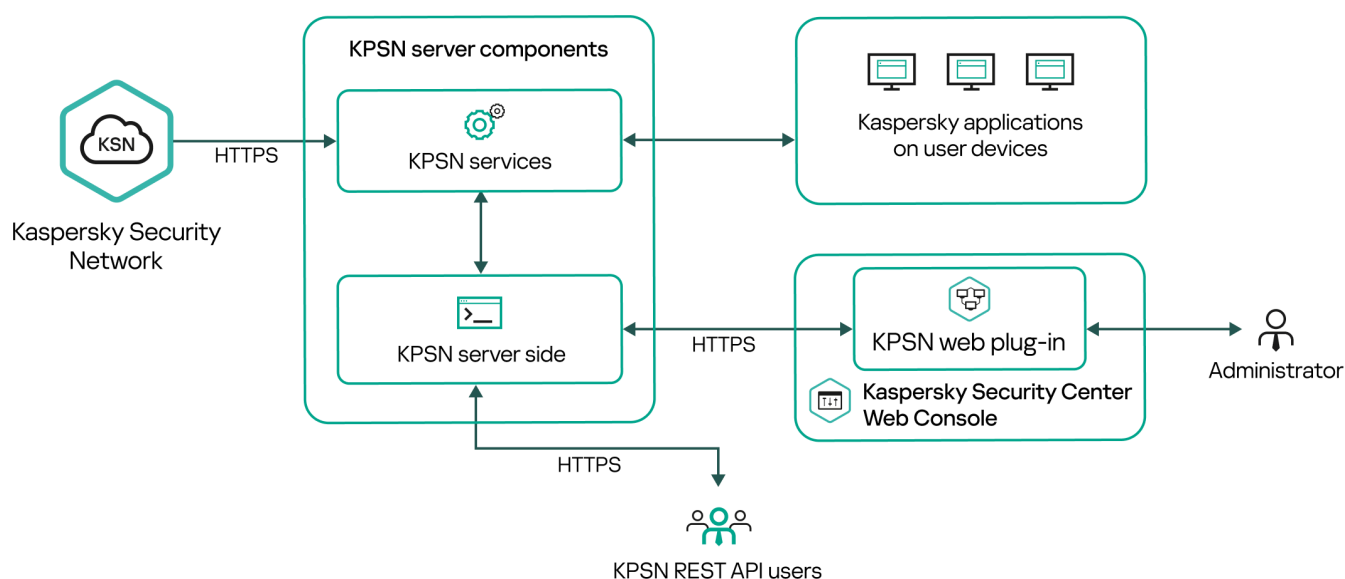
To deploy the server part of Kaspersky Private Security Network in the standard configuration, you need:

- A cluster on which you want to install all components of Kaspersky Private Security Network, except for the Gateway External and Gateway Internal components.

The Gateway External and Gateway Internal components are used only in a configuration with a unidirectional gateway.

- A server with Kaspersky Security Center installed, on which you will install the Kaspersky Private Security Network web plug-in. For details, see [Hardware and software requirements](#).

The standard deployment scenario of Kaspersky Private Security Network is shown in the figure below.



Standard deployment scenario of Kaspersky Private Security Network.

Kaspersky Private Security Network with a proxy server

Kaspersky Private Security Network configuration with a proxy server is used if access to Kaspersky Lab servers from the corporate LAN is only allowed through a proxy server provided by your organization. In such a case, the corporate LAN is divided into the [open](#) network segment and the [categorized](#) network segment, one of which includes the proxy server and the other includes the Kaspersky Private Security Network.

To deploy the server part of Kaspersky Private Security Network with a proxy server, you need:

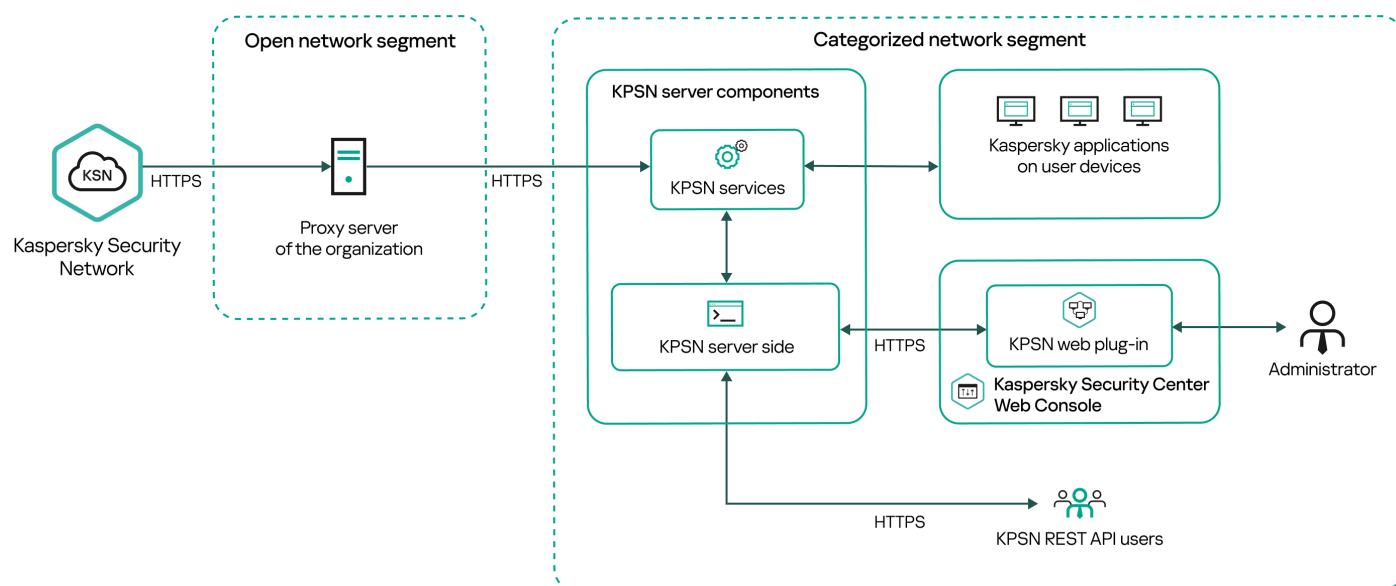
- A cluster in the categorized network segment. On cluster servers, you must install all components of the server part of Kaspersky Private Security Network, except for the Gateway External and Gateway Internal components.

The Gateway External and Gateway Internal components are used only in a configuration with a unidirectional gateway.

- A server in the open network segment on which your organization's proxy server is deployed.
- A server in the categorized network segment. On this server, you must deploy all components of Kaspersky Private Security Network, except for the Gateway External and Gateway Internal components.
- A server with Kaspersky Security Center installed, on which you will install the Kaspersky Private Security Network web plug-in. For details, see [Hardware and software requirements](#).

To ensure the interaction between Kaspersky Private Security Network and Kaspersky servers through the proxy server of your organization, you must [configure the proxy server](#) using the Kaspersky Private Security Network web plug-in.

The scenario for Kaspersky Private Security Network deployment with a proxy server is shown in the figure below.



Kaspersky Private Security Network deployment scenario with a proxy server

Kaspersky Private Security Network with a unidirectional gateway

Kaspersky Private Security Network configuration with a unidirectional gateway is used if access to Kaspersky servers is blocked on the corporate LAN. In such a case, the corporate LAN is divided into the open network segment and the categorized network segment, the communication between which is achieved using a unidirectional gateway. Kaspersky Private Security Network and Kaspersky Security Center Web Console must be installed in both network segments, but Kaspersky Private Security Network relies upon different components in different segments.

To deploy Kaspersky Private Security Network with a unidirectional gateway, you need at least two clusters:

- **Cluster 1** in the open network segment.

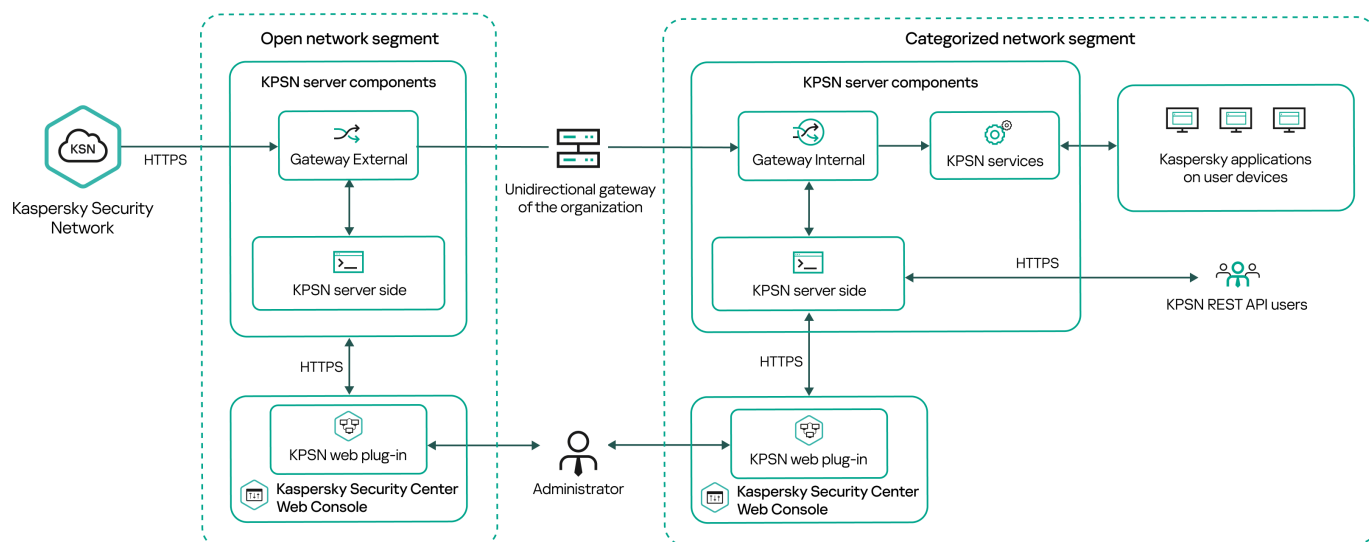
In cluster 1, you need to deploy the server part of Kaspersky Private Security Network and the Gateway External component. The Gateway External component can receive reputation database updates from Kaspersky servers over an encrypted link.

- **Cluster 2** in the categorized network segment.

In cluster 2, you must deploy the server part of Kaspersky Private Security Network, the Gateway Internal component, and other Kaspersky Private Security Network server components that you need. The Gateway Internal component can receive reputation database updates from the Gateway External component through the unidirectional gateway and forward them to other components of Kaspersky Private Security Network.

- Two servers, each of which has the Kaspersky Security Center application installed, in which you will install the Kaspersky Private Security Network web plug-in. For details, see [Hardware and software requirements](#). One server must be in the open network segment, and the other server must be in the categorized network segment.

The scenario for Kaspersky Private Security Network deployment with a unidirectional gateway is shown in the figure below.



Scenario of Kaspersky Private Security Network deployment with a unidirectional gateway

Deploying Kaspersky Private Security Network with redundancy

To help ensure the uninterrupted operation of the application, you can install multiple instances of Kaspersky Private Security Network components. For example, you can add multiple instances of the URL Reputation component when following [any deployment scenario](#) (standard, proxy, or unidirectional gateway).

The maximum number of instances of each component corresponds to the number of servers in the Kubernetes cluster.
There can be only one instance of the Gateway External and Gateway Internal components.

You can [configure the number of component instances](#) using the Kaspersky Private Security Network web plug-in.

Managing access permissions

You can manage access permissions for the functionality of Kaspersky Private Security Network in the Kaspersky Security Center Web Console (please refer to the *Kaspersky Security Center Help*).

For Kaspersky Private Security Network, you must set the following access permissions:

- API access
- Managing Kaspersky Private Security Network settings
- Managing the local file reputation database
- Managing the local website reputation database.

Adding or removing a server

Kaspersky Private Security Network components are deployed in a Kubernetes cluster. For information on adding a server to the cluster, please refer to the documentation of the k3s orchestrator.

Servers are also removed using the orchestrator. Before removing a server, make sure that the removal will not result in the number of instances of each component exceeding the number of servers remaining in the cluster.

After adding or removing a server, [Kaspersky Private Security Network service access addresses](#) should be updated:

- Add the address of the added server.
- Delete the address of the removed server.

Installing Kaspersky Private Security Network

Installation of Kaspersky Private Security Network consists of the following steps:

1. [Preparing to install Kaspersky Private Security Network](#)
2. [Installing the server part of Kaspersky Private Security Network](#).
3. [Getting an integration file for the Kaspersky Private Security Network web plug-in](#).
4. [Installing the Kaspersky Private Security Network web plug-in](#).

During installation of the web plug-in, it is integrated with the server part of Kaspersky Private Security Network.

Preparing to install Kaspersky Private Security Network

You must perform the following preparations before installing Kaspersky Private Security Network:

1. Make sure that the servers are inside the local network in accordance with [deployment scenario](#).
2. Make sure the servers satisfy the [hardware and software requirements](#).
3. Make sure that the [necessary inbound and outbound connections](#) are allowed.

We strongly recommend to close all ports other than those listed in the [List of ports for operation of Kaspersky Private Security Network](#) section.

4. If Kaspersky Private Security Network is being used with a unidirectional gateway, configure interaction with the unidirectional gateway (see below).
5. Make sure that the operating systems on the servers where the application components are to be installed have been fully updated.

Confidential information (such as application logs) is stored on Kaspersky Private Security Network servers. You are advised to provide additional security for Kaspersky Private Security Network servers. After configuring additional security measures, make sure that the connections required by the application are available.

Some settings of the Kaspersky Private Security Network web plug-in that are used for interaction with the server side of Kaspersky Private Security Network are stored in the Kaspersky Security Center storage. You can gain access to the storage through Kaspersky Security Center OpenAPI™. Kaspersky Private Security Network does not check the integrity of the plug-in data storage in Kaspersky Security Center. The administrator must take steps to restrict access to Kaspersky Security Center OpenAPI using the tools provided by Kaspersky Security Center, the operating system, or other means.

Configuring a unidirectional gateway in Kaspersky Private Security Network unidirectional gateway deployment scenario

The unidirectional gateway must be configured to transfer, for each stream you need, files from the `"/var/kpsn/gateway_external/<stream name>/data"` directory on the Gateway External server to the `"/var/kpsn/gateway_internal/<stream name>"` directory on the Gateway Internal server, and then delete the transferred files from the Gateway External server. The nested folder structure should be retained during the transfer of files. For this reason, only the files should be deleted, without deleting the folders.

The transferred files must have 0666 permissions.

If the unidirectional gateway supports configuration of the order of file transfer, it is recommended to transfer them in lexicographical order.

Installing the server part of Kaspersky Private Security Network

The server part of Kaspersky Private Security Network is installed using the `install.sh` installation script.

You must run the installation on the Control node of the Kubernetes cluster.

To install the server part of Kaspersky Private Security Network:

1. Unpack the `KPSN_install_<version>.tar.gz` archive.
2. Download the necessary third-party software:
 - For Kaspersky Private Security Network 4.0–4.0.4:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```
 - For Kaspersky Private Security Network 4.0.5 or later:

```
cd ./images/  
sudo -E ./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

You can download the third-party software to another computer, and then copy the downloaded objects to the corresponding folders of the extracted archive.

3. Configure the Kubernetes cluster to use a local container repository:

- a. Add the following line to the `/etc/hosts` file:

```
127.0.0.1 ksn-repo
```

- b. Create the `/etc/rancher/k3s/registries.yaml` file if it does not exist yet. Add the following lines to this file, making sure to observe the two-space indentation at the beginning of each line:

```
mirrors:
  "ksn-repo:31000":
    endpoint:
      - "http://ksn-repo:31000"
```

- c. Restart the k3s service using the following command:

```
sudo systemctl restart k3s.service
```

You must perform step 3 must on each server in the cluster.

4. Go to the directory with the extracted `KPSN_install_<version>.tar.gz` archive and run the installation script:

```
./install.sh
```

5. Read the terms and conditions of the End User License Agreement, which you can find in the directory indicated in the script output.

6. If you do not accept the terms of the End User License Agreement, you must abort the installation of the application and may not use the application.

7. If you accept the terms of the End User License Agreement, run the installation script with the `--accept-eula` option:

```
./install.sh --accept-eula
```

The script installs components required for the operation of Kaspersky Private Security Network, for example, Kubernetes packages. Wait for the script to finish.

If you are installing Kaspersky Private Security Network 4.0.1 or later, skip steps 8 through 9.

8. Copy the `kpsnctl` file from the archive to the `/usr/local/bin` directory on the server where you performed the previous step:

```
sudo cp ./kpsnctl /usr/local/bin
```

9. Set permissions for the file:

```
sudo chmod 755 /usr/local/bin/kpsnctl
```

The server part of Kaspersky Private Security Network is installed.

Preparing an integration file for the Kaspersky Private Security Network web plug-in

After the installation of the server part of Kaspersky Private Security Network is complete, you need to prepare the integration file of the Kaspersky Private Security Network web plug-in. The integration file includes the information required to establish a TLS connection between the server part of Kaspersky Private Security Network and the Kaspersky Private Security Network web plug-in. The integration file is prepared using the `kpsnctl` tool. You can find the `kpsnctl` utility in the installation archive of the server part of Kaspersky Private Security Network.

Before performing the instructions below, obtain the CSR file in the [Kaspersky Private Security Network web plug-in setup wizard](#) and copy that file to the server where the server part of Kaspersky Private Security Network is installed.

Multiple names may be specified in the commands below. If the Kubernetes cluster you are using includes multiple servers, you must specify at least one name for each server in the commands below. The `--external-hostname` option must precede each name.

Example of specifying multiple names:

```
kpsnctl certs rotate ca --external-hostname example1.com --external-hostname example2.com
```

To prepare an integration file for the Kaspersky Private Security Network web plug-in:

1. Generate certificate files for Kaspersky Private Security Network:

- If this is the first time integration, use the following command:

```
kpsnctl certs rotate ca --external-hostname <host name available from the server with Kaspersky Security Center installed>
```

- If the integration has been configured before, use the following command:

```
kpsnctl certs rotate server --external-hostname <host name available from the server with Kaspersky Security Center installed>
```

- If you want to rotate the certificate authority (CA) used by Kaspersky Private Security Network, use the following command:

```
kpsnctl certs rotate ca --force --external-hostname <host name available from the server with Kaspersky Security Center installed>
```

Executing the `kpsnctl certs rotate ca` command invalidates previously issued [certificates for the API](#).

If the server certificate expires, errors may occur when using the Kaspersky Private Security Network web plug-in and API. We recommend configuring regular rotation of the server certificate, for example, by using cron. To configure automatic rotation once a month, run the command:

```
(crontab -l 2>/dev/null; echo "0 0 1 * * kpsnctl certs rotate server --external-hostname <host name available from the server with Kaspersky Security Center installed>") | crontab -
```

2. Generate the integration file:

```
kpsnctl generate-integration-file --client-csr <path to the CSR file> --external-hostname <host name accessible from the Kaspersky Security Center server> > integration.json
```

You will need the obtained integration.json file to configure the integration in the [Kaspersky Private Security Network web plug-in setup wizard](#).

Installing the Kaspersky Private Security Network web plug-in

Installation of the web plug-in on Kaspersky Security Center virtual servers is not supported.

The Kaspersky Private Security Network web plug-in is installed in the web interface of Kaspersky Security Center Web Console.

You need the following files from the distribution kit:

- Installation ZIP archive with web plug-in files
- TXT file with the signature for verifying the installation ZIP archive

To start the Kaspersky Private Security Network web plug-in installation:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**. In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.
2. Add the Kaspersky Private Security Network web plug-in:
 - a. Click **Add from file**.
 - b. Click **Download ZIP file** to download the ZIP archive with the web plug-in files.
 - c. Click **Upload signature** to upload the TXT file with the signature.
 - d. Click **Add**.
 - e. Reload the page.

The Kaspersky Private Security Network web plug-in should appear in the list of web plug-ins.

If Kaspersky Private Security Network sections are not available in the web interface after you install the web plug-in, restart Kaspersky Security Center Web Console.

3. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

4. Click **Install KPSN**.

This opens the Kaspersky Private Security Network Setup Wizard. The following describes the steps of the setup wizard.

Step 1. Integration of the server part of Kaspersky Private Security Network and the Kaspersky Private Security Network web plug-in

The server part can be integrated only with one web plug-in at a time.

This step involves preparing for the integration of the server part of Kaspersky Private Security Network with the Kaspersky Private Security Network web plug-in.

Preparing for integration includes getting a certificate signing request file (CSR file) and an integration file, and checking their compatibility with each other.

To prepare the files necessary for integration:

1. Under **KPSN CSR**, click **Download** and get the CSR file.

While performing the following actions, do not close or refresh the page of the setup wizard on which you got the CSR file.

2. On the server where the server part of Kaspersky Private Security Network is installed, use the CSR file to [generate an integration file](#).
3. Go back to the Kaspersky Private Security Network web setup wizard.
4. Click the **Select file** button to upload the integration file that you got on the server with the server part of Kaspersky Private Security Network.

The setup wizard checks whether the information in the file matches the information about the previously received CSR file.

If you closed or refreshed the page of the setup wizard in the meantime, the data in the integration file will be incorrect. In this case, you must get a new CSR file and a corresponding integration file.

When you proceed to the next step, the server part of Kaspersky Private Security Network is integrated with the Kaspersky Private Security Network web plug-in. Integration may take several minutes, please wait until it finishes.

Step 2. Uploading the activation archive

At this step, you need to provide the activation archive that you got from Kaspersky. Click **Add files** to upload this archive to the setup wizard.

The setup wizard verifies the data in the archive. If no errors are found, you can go to the next step.

Step 3. Selecting components for installation

At this step, you can select the server components of Kaspersky Private Security Network that you want to install. On the card of each component, you can select the number of instances of the component that you want to install. More instances means higher performance of Kaspersky Private Security Network, but also greater usage of memory and disk space.

Depending on the number of selected components, the amount of disk space that you need is recalculated; information about this is displayed in the **Requirements** section.

Step 4. Installing components

At this step, you can check which components and how many instances are ready to be installed.

After making sure that the selection of components matches your requirements, click **Install**.

The setup wizard installs the selected components.

Step 5. Adding traffic encryption keys

At this step, you can add one or more traffic encryption keys.

Traffic encryption keys are needed to encrypt data transmitted between the Kaspersky Private Security Network services, and computers with Kaspersky applications installed.

You can add traffic encryption keys in the following ways:

- Generate a new key (the **Generate key** button)
- Import an existing key (the **Import key** button)

Step 6. Adding an installation ID

At this step, you specify the information that can be used to identify the installed Kaspersky Private Security Network:

- In the **KPSN installation name** field, enter any name of your choosing. This is a required setting.

The installation name is your unique ID for Kaspersky. You must use it to get updates and certificates.

Do not use a test name because the installation name cannot be changed later. The value entered here will be used for future updates.

- In the fields below, you can enter the addresses at which Kaspersky Private Security Network will be available to other Kaspersky applications.
 - In the **Addresses for internal access** field, specify the IP address or URL to be used for access inside the network that contains the KPSN server.
 - In the **Addresses for external access** field, enter the IP address or URL for access from the external network.

Only IPv4 addresses are supported.

Step 7. Checking the configuration

At this step, you can check the settings of the Kaspersky Private Security Network that you are installing.

Finishing the installation

After installation is complete, click **Finish setup and start KPSN**.

Updating Kaspersky Private Security Network

Updating Kaspersky Private Security Network to version 4.0.1 and later is available for Kaspersky Private Security Network versions 4.0 or later. Updates for each version are cumulative: for example, to update the server part of Kaspersky Private Security Network 4.0 to version 4.0.3, it is sufficient to install version 4.0.3, skipping the installation of versions 4.0.1 and 4.0.2.

The update procedure can include one of the following steps, or both:

- [Updating the Kaspersky Private Security Network web plug-in](#)
- [Updating the server part of Kaspersky Private Security Network](#)

If the update involves updating both the server part and the web plug-in, you must first install the update of the web plug-in, and then the update of the server part of Kaspersky Private Security Network.

You can view your current version of the Kaspersky Private Security Network web plug-in in the web interface of Kaspersky Private Security Network in the **KPSN** → **Settings** → **Web plug-ins** section (in Kaspersky Security Center Web Console 14.2, in the **Console settings** → **Web plug-ins** section).

You can view your current version of the server part of Kaspersky Private Security Network in the web interface of Kaspersky Private Security Network in the **KPSN** → **Settings** → **About KPSN** section (in Kaspersky Security Center Web Console 14.2, in the **Operations** → **KPSN Settings** → **About KPSN** section).

Updating the Kaspersky Private Security Network web plug-in

The Kaspersky Private Security Network web plug-in is updated in the web interface of Kaspersky Security Center Web Console.

You need the following files:

- Installation ZIP archive with web plug-in update files
- TXT file with the signature for verifying the installation ZIP archive

To update the Kaspersky Private Security Network web plug-in:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**.
In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.

2. Add the Kaspersky Private Security Network web plug-in:
 - a. Click **Update from File** to upload the web plug-in update from a file.
 - b. Specify the file and the signature of the file.
 - c. Upload the file.

The Kaspersky Private Security Network web plug-in is updated from the file and is displayed in the list of web plug-ins in the Kaspersky Security Center Web Console.

Updating the server part of Kaspersky Private Security Network

The server part of Kaspersky Private Security Network is updated using the `install.sh` installation script.

You must run the update on the Control node of the Kubernetes cluster. If multiple such nodes exist, we recommend selecting the node on which the Kaspersky Private Security Network installation procedure was performed.

To update the server part of Kaspersky Private Security Network:

1. Make sure that the [hardware and software requirements](#) are satisfied.
2. Unpack the `KPSN_install_<version>.tar.gz` archive.
3. Download the necessary third-party software:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

You can download the third-party software to another computer, and then copy the downloaded objects to the corresponding folders of the extracted archive.

4. Go to the directory with the extracted `KPSN_install_<version>.tar.gz` archive and run the script:
`./install.sh`
5. If the script prompts you to accept the End User License Agreement before letting you install the update:
 - a. Read the terms and conditions of the End User License Agreement, which you can find in the directory indicated in the script output.
 - b. If you do not accept the terms of the End User License Agreement, you must abort the installation of the application and may not use the application.

c. If you accept the terms of the End User License Agreement, run the installation script with the `--accept-eula` option:

```
./install.sh --accept-eula
```

The script installs the Kaspersky Private Security Network update.

Installing the update does not affect Kaspersky Private Security Network settings and databases.

Updating Kaspersky Private Security Network to version 4.0.1

The earliest version of Kaspersky Private Security Network that you can update to version 4.0.1 is version 4.0.

Updating Kaspersky Private Security Network to version 4.0.1 involves the following steps:

- 1 [Updating the Kaspersky Private Security Network web plug-in](#)
- 2 [Updating the server part of Kaspersky Private Security Network](#)

After the update, you will be using Kaspersky Private Security Network web plug-in version 11.0.33, and the server part of Kaspersky Private Security Network version 4.0.375.

Updating Kaspersky Private Security Network to version 4.0.2

Updating Kaspersky Private Security Network to version 4.0.2 is available for Kaspersky Private Security Network versions 4.0 and 4.0.1.

Updating Kaspersky Private Security Network from version 4.0 to version 4.0.2 involves the following steps:

- 1 [Updating the Kaspersky Private Security Network web plug-in](#)
- 2 [Updating the server part of Kaspersky Private Security Network](#)

To update Kaspersky Private Security Network from version 4.0.1 to version 4.0.2, you need to [update the server part of Kaspersky Private Security Network](#). Updating the web plug-in is not required.

After the update, you will be using Kaspersky Private Security Network web plug-in version 11.0.33, and the server part of Kaspersky Private Security Network version 4.0.430.

Updating Kaspersky Private Security Network to version 4.0.3

Updating Kaspersky Private Security Network to version 4.0.3 is available for Kaspersky Private Security Network version 4.0 and later.

To update Kaspersky Private Security Network to version 4.0.3

1. Make sure that you are using Kaspersky Private Security Network web plug-in version 11.0.33 (corresponds to version 4.0.1). To do so, do one of the following:
 - In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**.
 - In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.
2. If the version of the web plug-in is different, install the [web plug-in update](#) for version 4.0.1.
3. [Update the server part of Kaspersky Private Security Network](#).

Kaspersky Private Security Network is updated to version 4.0.3 After the update, you will be using version 4.0.527 of the server side of Kaspersky Private Security Network.

Updating Kaspersky Private Security Network to version 4.0.4

Updating Kaspersky Private Security Network to version 4.0.4 is available for Kaspersky Private Security Network version 4.0 and later.

To update Kaspersky Private Security Network to version 4.0.4:

1. Make sure that you are using Kaspersky Private Security Network web plug-in version 11.0.33 (corresponds to version 4.0.1). To do so, do one of the following:
 - In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**.
 - In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.
2. If the version of the web plug-in is different, install the [web plug-in update](#) for version 4.0.1.
3. Update the server part of Kaspersky Private Security Network:
 - a. Make sure that the [hardware and software requirements](#) are satisfied.
 - b. Unpack the KPSN_install_<version>.tar.gz archive.
 - c. Download the necessary third-party software:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

You can download the third-party software to another computer, and then copy the downloaded objects to the corresponding folders of the extracted archive.

d. Go to the directory with the extracted KPSN_install_<version>.tar.gz archive and run the script:

```
./upgrade.sh
```

e. If the script prompts you to accept the End User License Agreement before letting you install the update:

1. Read the terms and conditions of the End User License Agreement, which you can find in the directory indicated in the script output.
2. If you do not accept the terms of the End User License Agreement, you must abort the update and may not use the application.
3. If you accept the terms of the End User License Agreement, run the update script with the `--accept-eula` option:

```
./upgrade.sh --accept-eula
```

Kaspersky Private Security Network is updated to version 4.0.4

Installing the update does not affect Kaspersky Private Security Network settings and databases.

Updating Kaspersky Private Security Network to version 4.0.5

Updating Kaspersky Private Security Network to version 4.0.5 is available for Kaspersky Private Security Network version 4.0 and later.

Before the upgrade, we recommend **backing up your local reputation databases**.

To export data from the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Operations** → **KPSN reputation lists**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** section.

- If you want to export file reputation data, select the **File Reputation** tab.
- If you want to export URL reputation data, select the **URL Reputation** tab.

2. Click **Export list**:

- If you want to export information on trusted objects, select **Trusted**.
- If you want to export information on untrusted objects, select **Untrusted**.

Kaspersky Private Security Network downloads a file with a list of trusted or untrusted to the downloads folder specified in your browser settings. The list includes all objects that have been added to the local database and have not been deleted yet.

To update Kaspersky Private Security Network to version 4.0.6:

1. Make sure that you are using Kaspersky Private Security Network web plug-in version 11.0.33 (corresponds to version 4.0.1). To do so, do one of the following:

- In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**.
- In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.

2. If the version of the web plug-in is different, install the [web plug-in update](#) for version 4.0.1.

3. Update the server part of Kaspersky Private Security Network:

a. Make sure that the [hardware and software requirements](#) are satisfied.

b. Unpack the KPSN_install_<version>.tar.gz archive.

c. Download the necessary third-party software:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

You can download the third-party software to another computer, and then copy the downloaded objects to the corresponding folders of the extracted archive.

d. Go to the directory with the extracted KPSN_install_<version>.tar.gz archive and run the script:

```
./install.sh
```

e. If the script prompts you to accept the End User License Agreement before letting you install the update:

1. Read the terms and conditions of the End User License Agreement, which you can find in the directory indicated in the script output.
2. If you do not accept the terms of the End User License Agreement, you must abort the update and may not use the application.

3. If you accept the terms of the End User License Agreement, run the update script with the `--accept-eula` option:

```
./install.sh --accept-eula
```

Kaspersky Private Security Network is updated to version 4.0.5.

Installing the update does not affect Kaspersky Private Security Network settings and databases.

Updating Kaspersky Private Security Network to version 4.0.6

Updating Kaspersky Private Security Network to version 4.0.6 is available for Kaspersky Private Security Network version 4.0 and later.

Before the upgrade, we recommend **backing up your local reputation databases**.

To export data from the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Operations** → **KPSN reputation lists**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** section.

- If you want to export file reputation data, select the **File Reputation** tab.
- If you want to export URL reputation data, select the **URL Reputation** tab.

2. Click **Export list**:

- If you want to export information on trusted objects, select **Trusted**.
- If you want to export information on untrusted objects, select **Untrusted**.

Kaspersky Private Security Network downloads a file with a list of trusted or untrusted to the downloads folder specified in your browser settings. The list includes all objects that have been added to the local database and have not been deleted yet.

To update Kaspersky Private Security Network to version 4.0.6:

1. Make sure that you are using Kaspersky Private Security Network web plug-in version 1.1.0.33 (corresponds to version 4.0.1). To do so, do one of the following:

- In the web interface of Kaspersky Security Center Web Console 14.2, go to **Console settings** → **Web plug-ins**.
- In the web interface of Kaspersky Security Center Web Console of a different version, go to **Settings** → **Web plug-ins**.

2. If the version of the web plug-in is different, install the [web plug-in update](#) for version 4.0.1.

3. Remove [integration with the Kaspersky Private Security Network web plug-in](#).

4. Update the server part of Kaspersky Private Security Network:

a. Make sure that the [hardware and software requirements](#) are satisfied.

b. Unpack the KPSN_install_<version>.tar.gz archive.

c. Download the necessary third-party software:

```
cd ./images/  
./download_external_images.sh  
cd ./charts/  
./download_external_charts.sh
```

You can download the third-party software to another computer, and then copy the downloaded objects to the corresponding folders of the extracted archive.

d. Go to the directory with the extracted KPSN_install_<version>.tar.gz archive and run the script:

```
./install.sh
```

e. If the script prompts you to accept the End User License Agreement before letting you install the update:

1. Read the terms and conditions of the End User License Agreement, which you can find in the directory indicated in the script output.
2. If you do not accept the terms of the End User License Agreement, you must abort the update and may not use the application.
3. If you accept the terms of the End User License Agreement, run the update script with the `--accept-eula` option:

```
./install.sh --accept-eula
```

5. If you encounter issues while updating the Kaspersky Private Security Network server, such as the update process not progressing, follow these steps:

a. Find pods in the *Error* state in the kpsn namespace cluster by running the following command:

```
kubectl -n kpsn get pods | grep -i error
```

b. Use the following command to delete pods:

```
kubectl -n kpsn delete pod <pod_name1> <pod_name2>
```

c. Execute the server-side update script again (step 4d).

6. [Integrate the server part of Kaspersky Private Security Network with the Kaspersky Private Security Network web plug-in](#).

Kaspersky Private Security Network is updated to version 4.0.6.

Installing the update does not affect Kaspersky Private Security Network settings and databases.

Removing the integration with Kaspersky Private Security Network

You can remove the integration with Kaspersky Private Security Network on the current Administration Server.

You may need to remove the integration in the following cases:

- If you want to use a different Kaspersky Security Center Web Console server for Kaspersky Private Security Network.
- If you want to discontinue using the web plug-in or remove the web plug-in.
When removing the web plug-in, we recommend removing the web plug-in integration first. The web plug-in can be removed using Kaspersky Security Center Web Console tools. For more details, please refer to the *Kaspersky Security Center Web Console Help*.
- If Kaspersky Private Security Network encounters errors.

To remove the integration of the web plug-in and the server part of Kaspersky Private Security Network

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Settings** tab, under **Delete KPSN integration**, click **Delete integration with KPSN server**.
3. Confirm the action in the displayed window.

Integration with Kaspersky Private Security Network is removed on the current Administration Server.

After removing the integration, the Kaspersky Private Security Network web plug-in returns to its original state. Data of the server part and services of Kaspersky Private Security Network are not affected; Kaspersky Private Security Network services keep running. You can use the server part of Kaspersky Private Security Network on a different Kaspersky Security Center server by repeating the [integration procedure](#).

Removing Kaspersky Private Security Network

Removal of Kaspersky Private Security Network consists of the following steps:

1. Removing the server part of Kaspersky Private Security Network

To remove the server part, you can run the `./uninstall.sh` script from the installation archive of the server part of Kaspersky Private Security Network.

2. Removing the web plug-in

When removing the web plug-in, we recommend removing the web plug-in integration first. The web plug-in can be removed using Kaspersky Security Center Web Console tools. For more details, please refer to the *Kaspersky Security Center Web Console Help*.

Certificate for receiving updates

Kaspersky Private Security Network components need the update certificate to interact with Kaspersky servers to:

- [Receive database updates](#)
- [Receive configuration files](#)

The certificate is uploaded to Kaspersky Private Security Network as part of the activation archive when [configuring Kaspersky Private Security Network](#). Information about the status and expiration date of the update certificate is displayed in the following sections:

- In the web interface of Kaspersky Security Center Web Console 14.2, in the **Operations** → **KPSN settings** → **Configuration** section.
- In the web interface of Kaspersky Security Center Web Console of a different version, in the **Applications and services** → **KPSN** → **Settings** → **Configuration** section.

To get a new update certificate, please send a request to Kaspersky Technical Support. You will get an archive with the certificate to be imported into Kaspersky Private Security Network.

To import the update certificate archive into Kaspersky Private Security Network:

1. Contact [Technical Support](#) to request a new Kaspersky Private Security Network update certificate.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.
In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.
3. On the **KPSN configuration** tab, click **Certificate**.
This opens a window with details of the current certificate.
4. Click **Import new certificate**.
5. This opens a window; in that window, click **Browse** and select the archive you got from Kaspersky.
6. Click **Save**.

The new certificate is imported to Kaspersky Private Security Network.

Database update

Kaspersky Private Security Network gets database updates over HTTPS using an encrypted connection.

Database update for the simplified configuration

For a simplified configuration of Kaspersky Private Security Network, the following database update algorithm is used:

1. The Kaspersky Private Security Network service on your corporate LAN side sends an update request to the server at Kaspersky.
2. The server at Kaspersky uses the data from the request to determine if any updates are available.
3. The server at Kaspersky sends a response with database updates to your servers hosting Kaspersky Private Security Network services.

This algorithm is repeated for all update streams that your Kaspersky Private Security Network services need:

Updating databases for a configuration with a proxy server

In a configuration with a proxy server, Kaspersky Private Security Network sends requests and receives responses through the [proxy server specified by the administrator](#).

Updating databases for a configuration with a unidirectional gateway

In a configuration with a unidirectional gateway, database updates are handled by looped processes.

The Gateway External component receives database updates in the open network segment in accordance with the following algorithm:

1. Gateway External in the open segment of your corporate LAN sends a request to the server at Kaspersky asking for updates.
2. The server at Kaspersky uses the data from the request to determine if any updates are available.
3. The server at Kaspersky sends a response with database updates to the Gateway External server.
4. Gateway External writes the received updates to a file.

For Kaspersky Private Security Network with a unidirectional gateway, update streams are additionally packed into files for exchange between the Gateway External and Gateway Internal components. Database updates are transmitted between the open network segment and the categorized network segment in accordance with the following algorithm:

1. Your organization's unidirectional gateway moves files to the categorized network segment into a [directory used by Gateway External](#).
2. Gateway Internal writes updates from a file to an internal update stream.
3. The Kaspersky Private Security Network service in the categorized network segment gets updates from the internal stream.

In Kaspersky Private Security Network version 4.0.1 or higher, on the **Configuration** tab, in the cards of the Gateway Internal and Gateway External components, you can look up the server on which the relevant component is deployed. The directories used by the component are located on the specified server.

Service databases in the categorized network segment are updated in accordance with the following algorithm:

1. The Kaspersky Private Security Network service on your corporate LAN side sends an update request to the Gateway Internal server.
2. The Gateway Internal server uses data from the request to determine if any updates are available.
3. The Gateway Internal server sends a response with database updates to your servers hosting Kaspersky Private Security Network services.

Database update request

To update the databases, Kaspersky Private Security Network components send requests to Kaspersky servers.

Requests do not contain data on the infrastructure of the organization, data on local network computers, or other confidential information.

A request to Kaspersky contains the following data (the HTTPS protocol is used):

- Kaspersky Private Security Network installation ID that was created during installation of the server part of Kaspersky Private Security Network
- Kaspersky Private Security Network service ID
- Name of the database update stream
- Date of the last database update
- ID of the requested update message
- Number of update messages requested
- Request timeout

Monitoring database updates

You can monitor updates of Kaspersky Private Security Network databases to prevent malfunctions when updating data. If a stream update ends with an error, Kaspersky Private Security Network automatically repeats the update attempt.

To monitor database updates:

1. In the web interface of Kaspersky Security Center Web Console 14.2, select the **Monitoring & reporting** → **KPSN database update log** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Database update log** section.

2. Click the **Refresh** button to refresh the data.

You will see a table showing the data streams that were updated in Kaspersky Private Security Network.

Troubleshooting problems with data transfer via a unidirectional gateway

An error may occur when downloading reputation database packages from the open network segment to the categorized network segment via the unidirectional gateway. You can learn more about the error in the web interface of the categorized network segment of Kaspersky Private Security Network. If an error occurs, the web interface of the categorized network segment, in the **KPSN settings** section, on the **Configuration** tab, the  icon is displayed in the status of the Gateway Internal component.

To fix a database update loading error:

1. Open the web interface of the categorized network segment of Kaspersky Private Security Network.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

3. On the **Configuration** tab, click the **Gateway Internal** component.

This opens the **Data stream status** window. Data streams that encountered an error while loading are highlighted in red.

4. Write down or save the names of the data streams highlighted in red and their status codes.
5. Open the web interface of the open network segment of Kaspersky Private Security Network.
6. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.
In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

7. On the **Configuration** tab, click the **Gateway External** component.

This opens the **Update data stream** window.

8. In the **Stream** drop-down list, select the stream that encountered an error while loading.

9. In the **Status code** field, enter the code of the update stream that you obtained at step 4.

10. Click the **Refresh** button.

The download of the update stream resumes from the message corresponding to the entered value.

11. Repeat steps 8 to 10 for all data update streams that encountered a download error.

Configuring a proxy server

You can configure the interaction between Kaspersky Private Security Network components and Kaspersky servers to use a proxy server.

Kaspersky Private Security Network components interact with Kaspersky servers in the following cases:

- When getting [database updates](#)
- When requesting [configuration files through the web plug-in](#)

To configure a proxy server:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Settings** tab, under **Proxy server**, click **Configure connection**.
3. This opens a window; in that window, configure the proxy server connection settings:
 - a. If you want to use a proxy server, turn on the **Use proxy server** toggle switch.
You cannot configure proxy server settings if the toggle switch is turned off.
 - b. In the **Proxy server address** field, enter the address in the format of a DNS server name or an IPv4 address.
 - c. In the **Port** field, enter the port of the proxy server.
 - d. In the **Authentication** drop-down list, select the authentication type.
Possible values: **Do not authenticate**, **By login and password**.
 - e. If you have selected authentication by login and password, enter the authentication credentials in the **Login** and **Password** fields.
 - f. Click **Test connection** to see if you can connect to the proxy server.
 - g. If the specified settings are correct, click **Save**.

The proxy server connection is configured.

Kaspersky Private Security Network configuration

The configuration of Kaspersky Private Security Network is determined when you set up Kaspersky Private Security Network. The configuration includes:

- The installation name

This can only be specified during [setup](#).

- Kaspersky Private Security Network components

The components are installed when you [set up Kaspersky Private Security Network](#). You can [see what components are installed and how many](#) and, if necessary, [add or remove components](#).

- [Internal and external addresses for access to Kaspersky Private Security Network](#).

- Public traffic encryption keys.

You can add traffic encryption keys when you [set up Kaspersky Private Security Network](#). You can view information about the current traffic encryption keys or [add new encryption keys](#).

When changing the configuration of Kaspersky Private Security Network, you must [get a new configuration file](#) and apply it to applications that use Kaspersky Private Security Network.

Viewing information about the configuration

To view information about the Kaspersky Private Security Network configuration:

In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, select the **Applications and services** → **KPSN** → **Settings** section.

The following information is displayed on the **Configuration** tab:

- Kaspersky Private Security Network installation name
- Which components are installed and how many.
You can click a component to view information about it.
- [Status and expiration date of the certificate for getting Kaspersky Private Security Network updates](#).
- The status and expiration dates of [traffic encryption keys](#).

To view information about the current traffic encryption keys, you can click **Traffic encryption keys**.

Adding and removing components

To add or remove Kaspersky Private Security Network components:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click the component for which you want to change the number of instances.

This opens a window with component details.

3. In the **Quantity** field, enter the number of instances of the component that you want. To remove the component, set the value to 0.

To add components, you need more space on the server.

4. Click **Save**.

5. Confirm the addition or removal of the component in the confirmation window.

The Kaspersky Private Security Network component is installed or removed.

Information about installed components is displayed on the **Configuration** tab.

Getting Kaspersky Private Security Network configuration files

If you want Kaspersky applications to use Kaspersky Private Security Network, you need to get an archive with the Kaspersky Private Security Network server connection settings and import this archive into Kaspersky applications.

For example, when managing Kaspersky Security Center, you can configure it to use Kaspersky Private Security Network on the corporate LAN instead of Kaspersky Security Network.

For details on configuring Kaspersky applications to use Kaspersky Private Security Network, please refer to the documentation of the relevant applications.

Whenever you change the configuration of Kaspersky Private Security Network, you must create an archive with new configuration files and import it into Kaspersky applications that use Kaspersky Private Security Network.

The way of getting an archive with configuration files depends on the [deployment scenario of Kaspersky Private Security Network](#) and the place of the reconfigured Kaspersky Private Security Network instance in this scenario.

Standard configuration and configuration with a proxy server

To get configuration files for the current instance of Kaspersky Private Security Network:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Get configuration files for this KPSN instance**.

An archive with configuration files is downloaded to your computer.

Configuration with a unidirectional gateway

To get configuration files for Kaspersky Private Security Network in the categorized network segment:

1. In the web interface of Kaspersky Security Center Web Console 14.2 installed in the categorized network segment, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version installed in the categorized network segment, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Export configuration**.

3. This opens a window; in that window, click **Export**.

The configuration.json file is downloaded to your computer.

4. In the web interface of Kaspersky Security Center Web Console 14.2 installed in the open network segment, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version installed in the open network segment, go to the **Applications and services** → **KPSN** → **Settings** section.

5. On the **Configuration** tab, click **Get configuration files for KPSN behind gateway**.

6. This opens a window; in that window, select the configuration.json file obtained at step 2.

7. Click the **Get files** button.

An archive with configuration files is downloaded to your computer.

To get configuration files for Kaspersky Private Security Network in the open network segment:

1. In the web interface of Kaspersky Security Center Web Console 14.2 installed in the open network segment, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version installed in the open network segment, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Get configuration files for this KPSN instance**.

An archive with configuration files is downloaded to your computer.

Exporting the configuration if you failed to get configuration files

If you could not get configuration files using the methods described above, you can export the Kaspersky Private Security Network configuration and send the exported file to Kaspersky Technical Support.

To export the configuration:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Export configuration**.

3. This opens a window; in that window, click **Export**.

The configuration.json file is downloaded to your computer.

The following information is included in the request to get the configuration file:

- Kaspersky Private Security Network installation ID generated during installation
- Kaspersky Private Security Network version
- Configured internal and external access addresses of Kaspersky Private Security Network
- IDs of the installed Kaspersky Private Security Network components
- Public encryption keys for traffic between Kaspersky Private Security Network and applications that use Kaspersky Private Security Network, and information about their expiration dates

You must send the configuration file to Kaspersky. In a response, you will receive configuration files for configuring Kaspersky Private Security Network in other Kaspersky applications.

Encrypting traffic

Data transmitted between the Kaspersky Private Security Network server, Kaspersky Security Network server, and computers with Kaspersky applications installed must be encrypted. Traffic encryption keys are used for the encryption.

You can view information about the status and expiration dates of traffic encryption keys:

- To view information about an encryption key for the connection between Kaspersky Private Security Network servers and computers with Kaspersky applications, go to the **Operations** → **KPSN settings** → **Configuration** → **Traffic encryption keys** section.
- The validity period of the encryption key for the connection between Kaspersky Private Security Network servers and Kaspersky Security Network is the same as the validity period of the update certificate. To view the validity period of the update certificate, go to the **Operations** → **KPSN settings** → **Configuration** → **Certificate** section.

Traffic between Kaspersky Private Security Network servers and computers with Kaspersky applications

Ensuring traffic encryption involves of the following steps:

1 Adding a traffic encryption key for secure data exchange between Kaspersky Private Security Network servers and your organization's computers.

Encryption keys in Kaspersky Private Security Network are stored in the encryption key store. A traffic encryption key is valid for 1000 days.

You can add keys in the following ways:

- [Creating a key](#). The key is added automatically.
- [Adding an existing key](#) created with third-party software (for example, using the OpenSSL package).
- [Importing a previously exported key store](#).

2 [Getting configuration files for Kaspersky applications](#)

Configuration files with Kaspersky Private Security Network server connection settings contain public encryption keys.

3 Adding configuration files to Kaspersky applications

For details on configuring Kaspersky applications to use Kaspersky Private Security Network, please refer to the documentation of the relevant applications.

You can get private encryption keys from the Kaspersky Private Security Network server when exporting a key store.

Traffic between Kaspersky Private Security Network servers and Kaspersky Security Network

Traffic encryption is ensured by [uploading an activation archive](#).

Creating a traffic encryption key

To create a traffic encryption key:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Traffic encryption keys**.

3. This opens a window; in that window, click **Generate key**.

The traffic encryption key is created and automatically added to Kaspersky Private Security Network.

Adding a traffic encryption key

You can create private and public traffic encryption keys manually, e.g. using the OpenSSL package.

If you reinstall Kaspersky Private Security Network, the private encryption key will need to be re-added in the web interface of the application.

A private key must meet the following requirements:

- Length – 2048 bits.
- Format – DER or PEM.
- Algorithm – RSA.

Example creation of a key using an OpenSSL package:

```
openssl genrsa -out private.pem 2048
```

To add an existing traffic encryption key to Kaspersky Private Security Network:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Traffic encryption keys**.

3. This opens a window; in that window, click **Import key**.
4. Select a private key file.
5. Click the **Open** button.

The traffic encryption key is added to Kaspersky Private Security Network.

Exporting and importing the traffic encryption key store

To export the traffic encryption key store from Kaspersky Private Security Network:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Traffic encryption keys**.
3. This opens a window; in that window, click **Export encryption keys**.

All Kaspersky Private Security Network are downloaded to your computer in accordance with your browser settings in the form of a DAT file of the traffic encryption key store.

To import the key store to Kaspersky Private Security Network:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, click **Traffic encryption keys**.
3. Click **Import encryption keys**, and in the displayed window, select the DAT file of the key store.

The traffic encryption key store that you are importing must not be empty. At least one of the keys in the key store must not be expired.

4. Click the **Open** button.

The traffic encryption key store is uploaded to Kaspersky Private Security Network. The keys are deleted and replaced with the keys from the uploaded DAT file.

Kaspersky Private Security Network service access addresses

Kaspersky Private Security Network service access addresses are internal and external IP addresses or host names at which other Kaspersky applications can gain access to the Kaspersky Private Security Network services. Internal access addresses must belong to the same network in which the KPSN server is installed. External access addresses are addresses outside of this network.

Access addresses are part of the Kaspersky Private Security Network configuration. If access addresses change, you must [get a new configuration file](#) and apply it to applications that use Kaspersky Private Security Network.

If access addresses were specified during [setup](#), you can view the addresses in the **KPSN settings** section on the **Settings** tab, under **KPSN access addresses**.

To specify Kaspersky Private Security Network access addresses:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Settings** tab, under **KPSN access addresses**, click **Specify addresses**.

3. This opens a window; in that window, specify access addresses:

- a. If you want to specify an internal access address, on the **Internal access** tab, click **Add** and enter an IP address or host name.
- b. If you want to specify an external access address, on the **External access** tab, click **Add** and enter an IP address or host name.

Repeat the procedure to add as many addresses as you need. To remove an address from the list, click the  icon to the right of the address.

4. Click **Save**.

Access addresses are specified.

Managing local reputation databases

Kaspersky Private Security Network lets you flexibly utilize data from the File Reputation and URL Reputation services using local reputation databases.

A *local reputation database* is a database containing object (file or URL) reputation data, which is stored on a server with Kaspersky Private Security Network components installed, and not on Kaspersky Security Network servers. Local reputation databases are managed by the [administrator of Kaspersky Private Security Network](#). The information in the local reputation databases is only available to the company's computers.

The reputation of an object in the local reputation database has a higher priority than the reputation in Kaspersky Security Network. For example, if the local reputation database has the *Untrusted* reputation for the object, while Kaspersky Security Network has the *Trusted* reputation for the same object, the object shall have the *Untrusted* reputation for users in the corporate network (see figure below).

Procedure for managing local reputation databases

Local reputation databases should be managed by no more than one administrator at any given time, based on the following algorithm:

1. The Kaspersky Private Security Network administrator selects the file or website whose data must be added or changed in the local reputation database.
2. The Kaspersky Private Security Network administrator assigns the object one of the following reputation values: *Trusted* or *Untrusted*.
3. Kaspersky Private Security Network displays the information about the object's reputation received from Kaspersky Security Network databases, if any. Also displayed is the object reputation information previously assigned by the Kaspersky Private Security Network administrator.
4. The Kaspersky Private Security Network administrator makes a final decision on the object reputation and adds or modifies data in the local reputation database.
5. Kaspersky applications being used in your organization receive the updated object reputation data.

Best practices for assigning reputations to applications

Usually, the *Application Control* functionality of Kaspersky applications is sufficient to block or allow the launch of applications. Application Control allows you to configure access to application categories (for example, games) or individual applications based on metadata or other data. As a result, the application is prevented from being launched. See the *documentation for Kaspersky applications* for more details about how Application Control works.

You can also use the local reputation databases of the Kaspersky Private Security Network to prevent or allow the launch of applications. If you are using Kaspersky Private Security Network, applications with the *Untrusted* reputation are deleted rather than blocked. In addition, the use of local reputation databases comes with a number of special considerations (see below). For example, Kaspersky applications do not query the Kaspersky Security Network or Kaspersky Private Security Network for the reputation of the applications that are signed with a trusted Microsoft certificate. Thus, the reputation of applications that you have set in Kaspersky Private Security Network does not affect their operation.

If you are using your own applications which are not signed with a trusted certificate, you will need to assign the *Trusted* reputation to these applications. Assigning *Trusted* reputation includes the following steps:

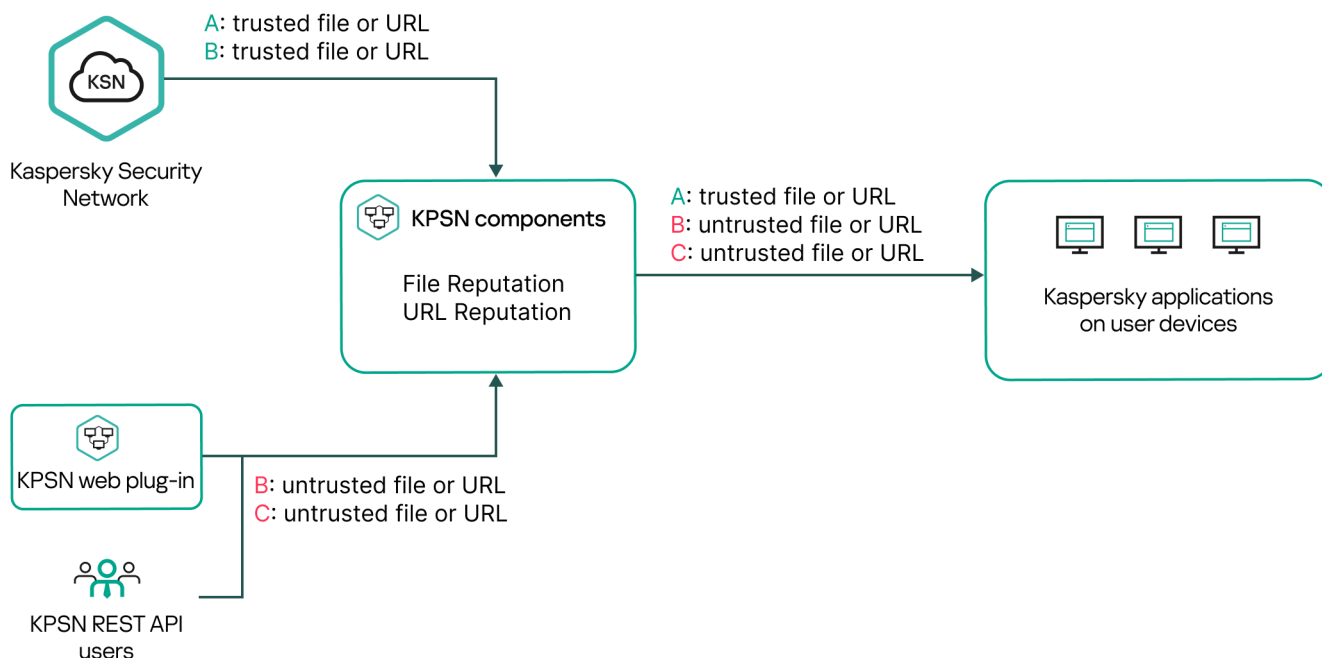
1. Add the details of your own application to your local reputation database.
2. In the settings of Kaspersky applications, add the following application category: KL category / Other applications / Applications trusted according to their assigned reputation in KSN.
3. In the Application Control settings, allow applications in the new category to be launched.

Special considerations for using local reputation databases

Kaspersky Private Security Network can be used with [various Kaspersky applications](#). The determined reputation of objects in local reputation databases can differ depending on the Kaspersky application installed on corporate computers. For example, object reputations determined by an application can vary for the following reasons:

- Kaspersky applications use *offline reputation databases* (hereinafter also referred to as the *offline databases*). Offline reputation databases include databases of trusted applications (*Microsoft System Critical Application*), trusted certificates (*Trusted Certificate*), and other data. Offline databases help optimize resources when running Kaspersky applications and protecting critical computer objects. Offline databases are created by Kaspersky experts based on Kaspersky Security Network data. Kaspersky applications keep their offline reputation databases updated. If information about an object is available in offline databases, the application does not query the reputation of the object in Kaspersky Security Network or Kaspersky Private Security Network.
- Exceptions are configured in application settings (trusted zone). In this case, the application does not take into account the reputation of the object in Kaspersky Private Security Network.
- The application uses scan optimization technologies, for example iSwift, iChecker, or caching of reputation queries in Kaspersky Security Network or Kaspersky Private Security Network. In this case, the application may avoid querying the reputation of the objects being scanned.
- The application queries reputation for files of certain formats only.
- The application does not query the reputation of large files.
- The application queries the reputation of an object in certain cases. For example, the application queries the reputation when running executable files, but does not query the reputation when scanning a file according to schedule.

For details on using local reputation databases Kaspersky corporate applications, please refer to the documentation of the relevant applications.



Procedure for managing local reputation databases by the Kaspersky Private Security Network administrator

Adding and updating file or URL reputation data

Kaspersky Anti Targeted Attack Platform allows adding file and website reputation data automatically. In this case, the *Untrusted* status is assigned to objects. For more details, please refer to the *Kaspersky Anti Targeted Attack Platform Administrator's Guide*.

You can add reputation information to the local reputation database of Kaspersky Private Security Network for one file or website at a time or for multiple files or websites at once.

To add or update the reputation information for a single file in the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN reputation lists** → **File Reputation** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** → **File Reputation** section.

2. Click **Add** and select the method for adding the file:

- **Add hash.**

For this option, you need the hash of the file (MD5 or SHA256).

- **Import file.**

For this option, you need the file for which you want to add a reputation record. The hashes of this file are calculated automatically.

3. In the opened window, specify the following information:

a. Under **Reputation**, select the reputation that you want to assign to the file. Possible values:

- **Trusted**
- **Untrusted**

b. If you selected the **Add hash** method, in the **Hash** field, enter the hash sum of the file.

Additionally, you can fill in the **File name** and **Description** fields. These fields are optional.

c. If you selected the **Import file** method, click **Browse**, select the certificate file, and click **Open**.

Additionally, you can fill in the **Description** field (optional).

4. Click **Save**.

This opens the Compliance Control window.

5. Compare the file reputation information from the Kaspersky Security Network database (the **KL reputation** column) and the information from the local reputation database (the **Current local reputation** column) with the newly added data (the **New local reputation** column). Decide whether you need to add new file reputation information (reputation update) to the local reputation database.

6. If you really want to update the file reputation in the local reputation database, click **OK**.

New data on the reputation of the selected file will be available for the Kaspersky applications being used in your organization.

To add or update the reputation information for multiple files in the local reputation database:

1. Prepare a list of files:

a. Create a text file (for example, list_for_import.txt).

b. Add a list of file hashes (MD5 or SHA256). In addition to the hash, you can enter a file name (up to 256 characters) and a description (up to 1024 characters). The hash, name and description of the file must be separated by a tab character. Each record must begin on a new line.

Example:

```
1BC29B36F623BA82AAF6724FD3B16718 file name description
AF6724FD3B167181BC29B36F623BA82A file name 2 description 2
```

The maximum supported number of records per file is 1000.

2. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN reputation lists** → **File Reputation** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** → **File Reputation** section.

3. Click **Import list**.

4. This opens a window; in that window:

a. Under **Reputation**, select the reputation that you want to assign to the file. Possible values:

- **Trusted**
- **Untrusted**

The reputation is assigned to all files in the list.

b. Import the TXT file with the list of files that you prepared at step 1. To do so, do one of the following:

- Drag the TXT file into the highlighted area.
- Click **Browse**, select the certificate file, and click **Open**.

5. Click **Import**.

This opens the Compliance Control window.

6. Compare the file reputation information from the Kaspersky Security Network database (the **KL reputation** column) and the information from the local reputation database (the **Current local reputation** column) with the newly added data (the **New local reputation** column). You may decide not to add new reputation information for some of the files in the local reputation database; in that case, clear the **Update** check box in the row of the file for which you do not want to update the reputation.

7. Click **OK**.

New data on the reputation of the added files will be available for the Kaspersky applications being used in your organization.

To add or update the reputation information for a website in the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN reputation lists** → **URL Reputation** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** → **URL Reputation** section.

2. Click **Add**.

3. In the opened window, specify the following information:

a. Under **Reputation**, select the reputation that you want to assign to the website. Possible values:

- **Trusted**
- **Untrusted**

- URL of the website. The URL must comply with RFC 3986.

When you add an URL to the local reputation database, all parts of the URL other than the domain and path are truncated. The "*" character is used as a wildcard to replace one or more characters.

- Description (optional).

4. Click **Save**.

This opens the Compliance Control window.

5. Compare the website reputation information from the Kaspersky Security Network database (the **KL reputation** column) and the information from the local reputation database (the **Current local reputation** column) with the newly added data (the **New local reputation** column). Decide whether you need to add new website reputation information (reputation update) to the local reputation database.

6. If you really want to update the website reputation in the local reputation database, click **OK**.

New data on the reputation of the selected URL will be available for the Kaspersky applications used in your organization.

To add or update the reputation information for multiple websites in the local reputation database:

1. Prepare a list of websites:

a. Create a text file (for example, list_for_import.txt).

b. Add a list of website URLs. In addition to an URL, you can enter a description of the website (up to 1024 characters). The URL and description must be separated by a tab character. Each record must begin on a new line.

```
Example:  
example.com description  
example2.com description 2
```

The maximum supported number of records per file is 1000. URL must comply with RFC 3986 standard, wildcard (*) can be used. When you add an URL to the local reputation database, all parts of the URL other than the domain and path are truncated. The "*" character is used as a wildcard to replace one or more characters.

2. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN reputation lists** → **URL Reputation** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** → **URL Reputation** section.

3. Click **Import list**.

4. In the opened window, specify the following information:

a. Under **Reputation**, select the reputation that you want to assign to the websites. Possible values:

- **Trusted**
- **Untrusted**

The reputation is assigned to all websites.

b. Import the TXT file with the list of websites that you prepared at step 1. To do so, do one of the following:

- Drag the TXT file into the highlighted area.
- Click **Browse**, select the certificate file, and click **Open**.

5. Click **Import**.

This opens the Compliance Control window.

6. Compare the website reputation information from the Kaspersky Security Network database (the **KL reputation** column) and the information from the local reputation database (the **Current local reputation** column) with the newly added data (the **New local reputation** column). You may decide not to add new reputation information for some of the websites in the local reputation database; in that case, clear the **Update** check box in the row of the website for which you do not want to update the reputation.

7. Click **OK**.

New data on the reputation of the added websites will be available for the Kaspersky applications used in your organization.

Exporting the local reputation database to a text file

To export data from the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Operations** → **KPSN reputation lists**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** section.

- If you want to export file reputation data, select the **File Reputation** tab.
- If you want to export URL reputation data, select the **URL Reputation** tab.

2. Click **Export list**:

- If you want to export information on trusted objects, select **Trusted**.
- If you want to export information on untrusted objects, select **Untrusted**.

Kaspersky Private Security Network downloads a file with a list of trusted or untrusted to the downloads folder specified in your browser settings. The list includes all objects that have been added to the local database and have not been deleted yet.

Deleting file or URL reputation records

Deleting file or website reputation records from the local reputation database means that the file or website reputation record becomes "disabled" and unavailable to Kaspersky applications used in your organization. A record about the file or website remains available in the web interface of the KPSN plug-in, you can enable it after deletion.

To delete records from the local reputation database:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Operations** → **KPSN reputation lists**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Reputation lists** section.

Then:

- If you want to delete file reputation data, select the **File Reputation** tab.
- If you want to delete URL reputation data, select the **URL Reputation** tab.

2. Disable the selected records in one of the following ways:

- In the rows of those records that you want to disable, in the **Status** column, set the toggle switch to **Disabled**.
- Select the check boxes in the rows of the records that you want to disable, then click the **Status** button and select **Disable**.

Information about the selected files or websites is deleted from the local reputation database and is no longer available to Kaspersky applications used in your organization.

Monitoring the operation of Kaspersky Private Security Network

This section provides information on monitoring the operation of Kaspersky Private Security Network in the web interface of the plug-in.

To view general information about the Kaspersky Private Security Network performance:

1. Open the web interface of Kaspersky Security Center Web Console in a browser window.
2. Go to the **Monitoring & reporting** → **Dashboard** section.

On the dashboard, the **KPSN overall status** widget displays the general health status of Kaspersky Private Security Network, its components and configuration.

You can click the names of settings in the left part of the **KPSN overall status** widget to go to relevant sections of the Kaspersky Private Security Network web plug-in and find out more about its performance or problems. You can also go to the section with Kaspersky Private Security Network monitoring charts by clicking the **Details** button in the lower part of the widget.

Monitoring the status of components and servers

Kaspersky Private Security Network automatically checks the status of its [components](#) and servers by monitoring the following parameters:

- Database lag for each of the data streams on each server
- Status of the installed Kaspersky Private Security Network components
- Validity period of traffic encryption keys used between Kaspersky Private Security Network and Kaspersky applications
- Validity period of the certificate authority (CA) used to issue certificates
- Validity period of the Kaspersky Private Security Network server certificate
- Expiration date of the Kaspersky Private Security Network update certificate.

To view the status of Kaspersky Private Security Network components:

1. Open the web interface of Kaspersky Security Center Web Console in a browser window.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Monitoring & reporting** → **KPSN charts**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Charts** section.

3. Select the **Overall status** tab.

The page displays a table of completed health checks for servers and components of Kaspersky Private Security Network with their results. The results in the table are refreshed every 30 seconds.

4. If necessary, filter the rows of the table of completed checks:

- To view the check results for specific servers, click the header of the **Server** column and select the servers that you want to see from the drop-down list.
- To find rows that contain specific text, enter the search text in the **Search** field on the right side above the table and press **Enter**.

The table displays only those rows that contain the specified text in at least one column. All cells are searched for the text.

The following information is displayed in the table of checks:

- **Server** is the IP address and port, or the name of the server, for a check of a specific server. If the check is for Kaspersky Private Security Network as a whole, the server is not specified.
- **Object** is the name of the Kaspersky Private Security Network component check: for example, by the name of a low-level component or update stream.
- **Status** is the result of the Kaspersky Private Security Network check. The value can be **OK** if no errors are detected, or the text of the detected error.

Monitoring the reputation of objects

You can view statistics of object reputation responses that the [File Reputation and URL Reputation components](#) have provided to requests from Kaspersky applications.

To view the statistics of responses from Kaspersky Private Security Network components to requests from Kaspersky applications:

1. Open the web interface of Kaspersky Security Center Web Console in a browser window.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Monitoring & reporting** → **KPSN charts**.
In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Charts** section.
3. Select the **Responses** tab.
4. In the drop-down list of time periods, select the time period for which you want to view information on the performance of components.

The integrated page displays charts for the [components of Kaspersky Private Security Network](#). Charts of statistics of File Reputation and URL Reputation component responses for the selected time period are located in the corresponding blocks. If you only have one of these components installed, the page displays a block of charts for that component only.

The response statistics page is available only if you have at least one of the File Reputation or URL Reputation components installed.

Each block displays the following information:

- Total number of requests to the component
- Number of responses about objects with good, bad, or unknown reputation received from the component and from the local reputation database
- Pie chart and histogram that visualize response statistics

In Kaspersky Private Security Network 4.0.1 or higher, you can enable automatic update of the displayed charts. To do this, turn on the **Auto update** toggle switch. The chart is automatically updated every 30 seconds in accordance with the selected interval. You can also update the displayed charts manually.

Pie chart of object reputation

You can use the pie chart to monitor the percentage ratio of the number of responses about objects with good, bad, or unknown reputation by the File Reputation or URL Reputation components and the local reputation database to the total number of responses.

You can select or clear the check boxes in the left part of the block next to the responses to have the chart display statistics only for responses with the selected reputation.

You can hide the pie chart by clearing the **Show pie chart** check box.

Histogram of object reputation responses

You can use the histogram to monitor the number of responses about objects with good, bad, or unknown reputation by the File Reputation or URL Reputation components and the local reputation database vs time.

The height and color of each bar reflects the number of responses in the time period. You can select or clear the check boxes in the left part of the block next to the responses to have the chart display statistics only for responses with the selected reputation.

Monitoring the request processing time

To monitor the health of components, you can look at the time it takes for Kaspersky Private Security Network components to process requests from Kaspersky applications.

To view the request processing time for Kaspersky Private Security Network components:

1. Open the web interface of Kaspersky Security Center Web Console in a browser window.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Monitoring & reporting** → **KPSN charts**.
In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Charts** section.
3. Select the **Request processing speed** tab.
4. In the drop-down list of time periods, select the time period for which you want to view information on the performance of components.

The integrated page displays charts for the [components of Kaspersky Private Security Network](#). Charts for each of the Kaspersky Private Security Network components that are installed on the server are displayed in the corresponding blocks. Charts and diagrams displayed depend on the Kaspersky Private Security Network configuration and connected data streams.

Each block displays the following information:

- Total number of requests processed
- Number of requests processed by the component within a certain amount of time or not processed due to an error
- Pie chart and histogram that illustrate request processing time statistics.

In Kaspersky Private Security Network 4.0.1 or higher, you can enable automatic update of the displayed charts. To do this, turn on the **Auto update** toggle switch. The chart is automatically updated every 30 seconds in accordance with the selected interval. You can also update the displayed charts manually.

Pie chart of request processing times

You can use the pie chart to monitor the percentage ratio of the number of requests to the component processed within a certain time or not processed due to an error to the total number of requests to the component.

You can select or clear the check boxes in the left part of the block next to the time intervals to display statistics only for requests processed within that time.

Histogram of request processing speed vs time

You can use the histogram to monitor the number of requests to the component processed within a certain time or not processed due to a certain error for the selected period.

The height of each column represents the total number of requests during the specified period (both processed or not processed due to an error), and the color represents the number of requests that were processed or not processed within the specified time. You can select or clear the check boxes in the left part of the block next to the time intervals to display statistics only for requests processed within that time.

Request processing speed

You can use the charts to assess the performance of Kaspersky Private Security Network components by looking at the speed with which they process requests. The chart areas are filled with colors corresponding to the colors specified in the time period description area.

Monitoring the database lag

To monitor the lag of updated databases of Kaspersky Private Security Network components:

1. Open the web interface of Kaspersky Security Center Web Console in a browser window.
2. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Monitoring & reporting** → **KPSN charts**.
In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Charts** section.
3. Select the **KPSN database update** tab.
4. In the drop-down list of time periods, select the time period for which you want to view information on the performance of components.

The integrated page displays charts of database lag of Kaspersky Private Security Network services.

Charts for each of the Kaspersky Private Security Network components that are installed on the server are displayed in the corresponding blocks. Charts and diagrams displayed depend on the Kaspersky Private Security Network configuration.

You can use the chart to see the lag between the Kaspersky Private Security Network databases and the Kaspersky Security Network databases, which lets you monitor the connection quality. The height of each point on the chart represents the lag between the local reputation database of the component and the Kaspersky Security Network.

If you have installed multiple identical components of Kaspersky Private Security Network, these components are displayed as separate lines on the same chart. The caption of each line indicates the server name. You can use these lines to compare the packet receipt lag between components of the same type. You can clear the check boxes in the lower part of the chart to hide the lines of components on other servers.

In Kaspersky Private Security Network 4.0.1 or higher, you can enable automatic update of the displayed charts. To do this, turn on the **Auto update** toggle switch. The chart is automatically updated every 30 seconds in accordance with the selected interval. You can also update the displayed charts manually.

Troubleshooting Kaspersky Private Security Network components

This section contains information on the methods that are used to resolve possible problems with the operation of Kaspersky Private Security Network.

Problems with traffic encryption keys

To fix problems with traffic encryption keys:

1. Upload or create a new [traffic encryption key](#).
2. [Get a new Kaspersky Private Security Network configuration file](#) and apply it to applications that use Kaspersky Private Security Network.

Problems with update certificates

To solve problems with update certificates:

[Request a new certificate](#) from Kaspersky (in accordance with the license of your organization).

Problems associated with component activity

To troubleshoot problems associated with component activity:

Make sure the server satisfies the [hardware requirements](#).

Problems related to database update lag

To fix the issues related to database update lag:

1. Make sure the server satisfies the [hardware requirements](#).
2. Make sure that the certificate for communication with Kaspersky Security Network has not expired.
3. Make sure that the Kaspersky update servers are accessible.

Problems associated with the quality of query processing

To fix the problems associated with the quality of query processing:

1. Make sure the server satisfies the [hardware requirements](#).
2. Make sure that the number of applications connected to Kaspersky Private Security Network [matches the configuration](#).
3. Make sure that the versions of products that are connected to Kaspersky Private Security Network are supported.

Notifications about Kaspersky Private Security Network events

You can configure the following types of notifications:

- Email notifications about Kaspersky Private Security Network events
- Adding a Kaspersky Private Security Network event record to Syslog

If you want to receive email notifications, take steps to prepare an SMTP server.
If you want to keep records in syslog, take steps to prepare a syslog server.

Notifications can be generated for the following types of events:

- Expiration of traffic encryption keys.

An alert is generated if a traffic encryption key has expired or will expire in less than two weeks.

- Expiration of certificates

A notification is generated in the following cases:

- An update certificate has expired or will expire in less than two weeks.
- The Kaspersky Private Security Network server certificate has expired or will expire in less than a month.
- The validity period of the certificate authority used to issue certificates has expired or will expire in less than a month.

- Errors of KPSN components.

An alert is generated if a component terminated suddenly and did not go up within two minutes, or if more than one sudden terminations occurred within two minutes.

- Database lag.

An alert is generated if the service database lag threshold is exceeded.

- Request processing errors.

A notification is generated if errors occurred when processing requests from applications that use Kaspersky Private Security Network.

Configuring email notifications about Kaspersky Private Security Network events

If you want to receive email notifications, take steps to prepare an SMTP server.

To configure email notifications about Kaspersky Private Security Network events:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Notifications** tab, in the **Notifications** section, in event table, in the **Email** column, select check boxes in the rows of events for which you want to receive notifications.

3. In the **Mail server settings** section, click **Settings** to configure the mail server connection settings.

4. This opens the **Mail server settings** window; in that window, specify the email notification settings:

- a. In the **SMTP server address** field, enter your organization's mail server address (for example, `smtp.example.com`).

- b. In the **SMTP server port** field, enter the port of your organization's mail server (for example, 25).

- c. In the **Client authentication** drop-down list, select the authentication type.

Possible values: **Do not authenticate**, **By login and password**, **By certificate**.

- d. If you have selected authentication by login and password, enter the authentication credentials in the **Login** and **Password** fields.

- e. If you selected authentication by certificate:

1. In the **Client certificate format** drop-down list, select the certificate file format that you want to use for authentication.

2. In the **Client certificate password** field, enter the certificate password. This field is optional.

3. Click **Browse** and select a certificate file with the CRT, CER, PEM, or DER extension.

4. If you selected the **X.509** certificate format, click **Browse** and select a private key file in the KEY or PEM format.

- f. In the **TLS version** drop-down list, select the version of TLS that you want to use when connecting to the mail server.

Possible values: **Do not use TLS**, **Use TLS 1.2 or later**.

If you do not want to use the TLS protocol, select **Do not use TLS**. This value is available only if **Client authentication** is set to **Do not authenticate**.

- g. If you chose to use the TLS protocol, click **Browse** and select a trusted certificate file of the mail server.

If you enabled use of the TLS protocol, mail notifications are forwarded by the mail submission agent (MSA). However, the SMTPS protocol is not supported.

- h. In the **Sender email** field enter the email address or name that you want to use as the sender of the email notification.

i. In the **Language** field, select the language to be used for notifications.

j. Click **Save**.

5. To test the connection with the mail server, click **Send test email**, and in the displayed window, enter an email address at which you can receive the test email, then click **Send test email**.

If the message does not arrive, check the mail server settings and try sending the message again.

6. Specify the recipients of email notifications about Kaspersky Private Security Network events:

a. Click **Specify recipients**.

b. In the **Notification recipients** field, enter email addresses of notification recipients. You can add multiple addresses using a comma (,) or semicolon (;) as a delimiter.

c. Click **Save**.

Email notifications about Kaspersky Private Security Network events are configured.

Configuring the logging of Kaspersky Private Security Network events in Syslog

If you want to keep records in Syslog, take steps to prepare a Syslog server.

To configure the logging of Kaspersky Private Security Network events in Syslog:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Notifications** tab, in the **Notifications** section, in event table, in the **Syslog** column, select check boxes in the rows of events for which you want to receive notifications.

3. Under **Syslog settings**, click **Settings**.

4. This opens a window; in that window, configure the connection to the Syslog server:

a. In the **Address** field, enter the URL or IPv4 address of the Syslog server.

b. In the **Port** field, enter the port for connecting to the Syslog server.

c. In the **Protocol** field, specify the protocol used for the connection. Possible values: **UDP**, **TCP**.

d. Click **Save**.

Information about Kaspersky Private Security Network events is logged in Syslog with the *KPSN* tag.

The format of Kaspersky Private Security Network component error notifications to be added to Syslog is as follows: <date and time> <server address> kpsn <error message>.

Depending on the operating system of the server and its configuration, the process ID may not be logged in Syslog.

KPSN API

The *Kaspersky Private Security Network programming interface* (hereinafter also referred to as the "KPSN API" or simply the "API") is a set of REST components that lets you send requests to Kaspersky Private Security Network from any computer on the corporate LAN without using a browser. The API lets you identify a specific user for administering local reputation databases. Moreover, the user does not need the web interface of Kaspersky Private Security Network. To administer the databases, the user must obtain [permissions for managing local reputation databases](#).

API requests must be made over HTTPS. Client certificates are used for user authentication.

Using the API, you can do the following:

- Add file or website reputation data to local reputation databases.
- Delete file or website reputation data from local reputation databases.
- Check the reputation of individual files or websites.

One request may contain no more than 1000 items.

To send requests, a REST client (for example, Insomnia) must be installed on the computer. You can also send requests using a command line interpreter (for example, cURL).

Getting started with the API

To start using the KPSN API:

1. Make sure your account has access to the API.

If you plan to edit file or website reputation information, you also need access to managing the local file and website reputation database.

[You can manage access permissions in Kaspersky Security Center Web Console.](#)

2. Get certificates and a client authentication key:

- a. In the web interface of Kaspersky Security Center Web Console 14.2, go to **Operations** → **KPSN settings** → **API access**.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** → **API access** section.

- b. Click **Get API certificate**.

Kaspersky Private Security Network downloads a ZIP archive to the default folder for downloads.

The downloaded archive contains the following files:

- *client_certificate.pem* is your client certificate for using the API.
- *private_key.pem* is your private key for using the API.
- *ca_certificate.pem* is the public CA certificate. You can use it to verify the certificate of the Kaspersky Private Security Network server.

3. Look up the addresses at which the KPSN API is available.

These addresses are specified in the **API access** section, under **API access options**. You can use any of the addresses listed there.

Making API requests

To make API requests:

1. Unpack the previously [downloaded ZIP archive with the certificate and key](#) to the computer from which you will be making API requests.
2. Add your client certificate (*client_certificate.pem*) and the private key (*private_key.pem*) to the authentication settings of your REST client if you do not want to pass them in the requests themselves.
3. If necessary, add the public CA certificate (*ca_certificate.pem*) to the list of CAs used by your REST client.

Each request to the API must include the "Content-Type: application / json" header.

Example of a request with a key and certificate

```
curl --cert <certificate> --key <key> -X POST -H "Content-Type: application/json" -d  
<data> <KPSN API Address>
```

Where:

<certificate> is the path to your client certificate.

<key> is the path to your private key.

<data> is the request body in JSON format, examples are given in the following sections.

<KPSN API Address> is the KPSN address at which the API is available.

Adding file reputation data

Request

A request to add file reputation data contains the following parameters:

- `action` – request to perform actions with Kaspersky Private Security Network (value: `add_file`).
- `data.hash_type` – hash algorithm. Possible values:
 - `sha256`
 - `md5`

You can specify only one hash algorithm in a request (for example, only SHA256). If the file's hash does not match the value of `data.hash_type`, the request will not be processed and the response contains the `203 hash type mismatch` error.

- `data.force` – parameter indicating how to resolve conflicts when adding file reputation data (required parameter). Kaspersky Private Security Network checks for file reputation data previously added to the local reputation database and the data in the Kaspersky Security Network database (KL reputation). Possible values:
 - `true` – always change the current reputation to the reputation in the request.
 - `false` – change the current reputation to the reputation in the request only if Kaspersky Private Security Network does not have reputation data about the file. If reputation data about the file were already added to Kaspersky Private Security Network, the reputation is not changed. Default value.
- `data.hashes` (array):
 - `data.hashes.hash` – file hash: MD5 (16-byte string) or SHA256 (32-byte string).
 - `data.hashes.reputation` – file reputation. Possible values:
 - `1` – trusted;
 - `2` – untrusted.
 - `data.hashes.file_name` – file name (string up to 256 characters long).
 - `data.hashes.description` – additional description of the file (string up to 1024 characters long).

To add file reputation data:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.

3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.
5. Send the request to the File Reputation service.

The window of the REST client displays the response with the results of performing the request.

Example of a request body

```
{
  "action": "add_file",
  "data": {
    "hash_type": "sha256",
    "force": false,
    "hashes": [
      {
        "hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
        "reputation": 1,
        "file_name": "file1.exe",
        "description": "trust file, sha256 hash"
      },
      {
        "hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307204",
        "reputation": 2,
        "file_name": "file2.exe",
        "description": "untrust file, sha256 hash"
      }
    ]
  }
}
```

Response

The response contains the following information:

- `data.hash` – file hash (array): MD5 (16-byte string) or SHA256 (32-byte string).
- `data.publish_status` – result of performing the request. Possible values:
 - `true` – file data were successfully added to the local reputation database.
 - `false` – file data could not be added to the local reputation database. The local reputation database already contains data about the file. To change the file data, the parameter `data.force` must be set equal to `true`.

Example of a response

```
{
```

```

"data": [
{
"hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
"publish_status": true
},
{
"hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307204",
"publish_status": false
}
]
}

```

Adding URL reputation data

Request

A request to add URL reputation data contains the following parameters:

- **action** – request to perform actions with Kaspersky Private Security Network (value: `add_url`).
- **data.force** – parameter indicating how to resolve conflicts when adding URL reputation data (required parameter). Kaspersky Private Security Network checks for URL reputation data previously added to the local reputation database and the data in the Kaspersky Security Network database (KL reputation). Possible values:
 - `true` – always change the current reputation to the reputation in the request.
 - `false` – change the current reputation to the reputation in the request only if Kaspersky Private Security Network does not have reputation data about the URL. If reputation data about the URL were already added to Kaspersky Private Security Network, the reputation is not changed. Default value.
- **data.urls** (array):
 - **data.urls.url** – URL of the website. A URL must comply with the RFC 3986 standard, and a mask (*) can be used. When you add an URL to the local reputation database, all parts of the URL other than the domain and path are truncated. The "*" character is used as a wildcard to replace one or more characters.
 - **data.urls.reputation** – website reputation. Possible values:
 - `1` – trusted;
 - `2` – untrusted.
 - **data.urls.description** – additional description of the URL (string up to 1024 characters long).

To add a website reputation data:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.

3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.
5. Send the request to the URL Reputation service.

The window of the REST client displays the response with the results of performing the request.

Example of a request body

```
{
  "action": "add_url",
  "data": {
    "force": false,
    "urls": [
      {
        "url": "website1.com",
        "reputation": 1,
        "description": "social network"
      },
      {
        "url": "website2.com",
        "reputation": 2,
        "description": "network game"
      }
    ]
  }
}
```

Response

The response contains the following information:

- `data.url` – URL of the website (array).
- `data.publish_status` – result of performing the request. Possible values:
 - `true` – URL data were successfully added to the local reputation database.
 - `false` – URL data could not be added to the local reputation database. The local reputation database already contains data about the URL. To change the URL data, the parameter `data.force` must be set equal to `true`.

Example of a response

```
{
  "data": [
    {
      "url": "website1.com",
```

```

    "publish_status": true
  },
  {
    "url": "website2.com",
    "publish_status": false
  }
]
}

```

Deleting file reputation data

Request

A request to delete file reputation data contains the following parameters:

- `action` – request to perform actions with Kaspersky Private Security Network (value: `delete_file`).
- `data.hash_type` – hash algorithm. Possible values:
 - `sha256`
 - `md5`

You can specify only one hash algorithm in a request (for example, only SHA256). If the file's hash does not match the value of `data.hash_type`, the request will not be processed and the response contains the `203 hash type mismatch` error.

- `data.hashes` – file hashes (array): MD5 (16-byte string) or SHA256 (32-byte string).

To delete file reputation data:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.
3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.
5. Send the request to the File Reputation service.

The window of the REST client displays the response with the results of performing the request.

Example of a request body

```

{

```

```

"action": "delete_file",
"data": {
  "hash_type": "sha256",
  "hashes": [
    "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
  ]
}
}

```

Response

The response contains a hash of the deleted files, or an error code and description if the request failed.

Example of a response

```

{
  "data": [
    {
      "hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
    }
  ]
}

```

Deleting URL reputation data

Request

A request to delete URL reputation data contains the following parameters:

- **action** – request to perform actions with Kaspersky Private Security Network (value: `delete_url`).
- **data.urls** – URLs of the websites (array). The URLs must comply with RFC 3986. When you add an URL to the local reputation database, all parts of the URL other than the domain and path are truncated. The "*" character is used as a wildcard to replace one or more characters.

To delete a website reputation data:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.
3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.

5. Send the request to the URL Reputation service.

6. The window of the REST client displays the response with the results of performing the request.

Example of a request body

```
{
  "action": "delete_url",
  "data": {
    "urls": [
      "website1.com"
    ]
  }
}
```

Response

The response contains the URLs of the deleted websites, or an error code and description if the request failed.

Example of a response

```
{
  "data": [
    {
      "url": "website1.com"
    }
  ]
}
```

Verifying the reputation of files

Request

A request to verify the reputation of a file contains the following parameters:

- `action` – request to perform actions with Kaspersky Private Security Network (value: `check_file`).
- `data.hash_type` – hash algorithm. Possible values:
 - `sha256`
 - `md5`

You can specify only one hash algorithm in a request (for example, only SHA256). If the file's hash does not match the value of `data.hash_type`, the request will not be processed and the response contains the 203 hash type mismatch error.

- `data.hashes` – file hashes (array): MD5 (16-byte string) or SHA256 (32-byte string).

To check file reputation:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.
3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.
5. Send the request to the File Reputation service.

The window of the REST client displays the response with the results of performing the request.

Example of a request body

```
{
  "action": "check_file",
  "data": {
    "hash_type": "sha256",
    "hashes": [
      "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203"
    ]
  }
}
```

Response

Based on the file reputation response, you can assess the safety of using the file. The response contains the following information:

Parameter	Description	Always present in a response
hash	File hash (array): MD5 (16-byte string) or SHA256 (32-byte string).	Yes
reputation	File reputation. Possible values: • 0 – unknown; • 1 – trusted; • 2 – untrusted; • -1 – undefined.	Yes
description	More file reputation data.	No
product	Name of the application associated with the file.	No
vendor	Name of the file publisher.	No

Parameter	Description	Always present in a response
users	Number of Kaspersky Security Network users who are using this file (only for trusted files)	No
firstRequest	Date and time when the file became known to Kaspersky Security Network.	No
groupSharing	Percentage distribution of a file by trust level groups for Kaspersky applications reporting data to the Kaspersky Security Network. Trust level groups: • trusted; • untrusted; • low – strong restrictions; • high – weak restrictions.	No
geoSharing	Percentage distribution of file encounters by country. Countries are specified as a two-character code. 00 means statistics for multiple countries combined into one category.	No
client_data	Information source ID in the response: • true – reputation data from your organization sources; • false – reputation from Kaspersky Private Security Network databases.	Yes

Example of a response:

```
{
  "data": [
    {
      "hash": "9279fa6a314fb0728f7cfd93669cf7f35cc01b6389fd220664919f455b307203",
      "reputation": 2,
      "firstRequest": "1601-00-01T00:00:01Z",
      "users": 123,
      "product": "program",
      "vendor": "company",
      "client_data": "true",
      "groupSharing": {
        "high": 30,
        "low": 20,
        "trusted": 10,
        "untrusted": 40
      },
      "geoSharing": {
        "fr": 25,
        "it": 19,
        "uk": 15,
        "es": 12,
        "mx": 10,
        "00": 17
      }
    }
  ]
}
```

Verifying the reputation of websites

Request

A request to verify the reputation of a URL contains the following parameters:

- `action` – request to perform actions with Kaspersky Private Security Network (value: `check_url`).
- `data.urls` – URLs of the websites (array). The URLs must comply with RFC 3986.

To verify the reputation of a website:

1. Start the REST client on any computer on the corporate LAN that has access to the server at the address used by Kaspersky Private Security Network.
2. In the list of methods, select the POST method.
3. In the request address field, enter the address at which the KPSN API is available.
4. In the workspace, enter the body of the request in JSON format. See the example below.
5. Send the request to the URL Reputation service.

The window of the REST client displays the response with the results of performing the request.

Example of a request body

```
{
  "action": "check_url",
  "data": {
    "urls": [
      "website1.com"
    ]
  }
}
```

Response

Based on the website reputation response, you can assess the safety of visiting the website. The response contains the following information:

Parameter	Description	Always present in a response
url	data.url – website URL (array).	Yes
reputation	Website reputation. Possible values: • 0 – unknown; • 1 – trusted; • 2 – untrusted; • -1 – undefined.	Yes
ttl	Recommended time (in seconds), for which a customer can cash the response received	Yes
categories	List of website category IDs. If there is no data at the specified URL, an empty list will be returned.	Yes
client_data	Information source ID in the response: • true – reputation data from your organization sources; • false – reputation from Kaspersky Private Security Network databases.	Yes

Example of a response:

```
{
  "data": [
    {
      "url": "website1.com",
      "reputation": 1,
      "categories": [
        3,
        5,
        8
      ],
      "ttl": 3600,
      "client_data": "true"
    }
  ]
}
```

Error codes

While working with the API, you may receive errors from Kaspersky Private Security Network. Each error is assigned a code (see the table below). All errors are contained in the response body, except for error 401.

Error codes

Error code	Description (error category)	Recommendations
1	Required parameters are missing (general).	Verify that the request is entered correctly. Be sure that all required parameters are included in the request and that the parameters are correctly specified.
2	Invalid parameter type (general).	Verify that the request is entered correctly. Be sure that all parameter values are correctly specified.
3	Syntax error in request (general).	Verify that the request is entered correctly. For example, the value of the action might be set as check_url instead of chec1_url.
4	Invalid JSON code (general).	Verify that the request is entered correctly. For more information about the JSON format, see reference materials on JSON ADF scripts.
5	Duplicate request (general).	Verify that the request is entered correctly. You may have already sent this request.

Error code	Description (error category)	Recommendations
6	Too many records in the request (general).	Make sure that the request contains no more than 1000 records. Split the request if necessary.
51	The user does not have sufficient permissions (authorization).	Make sure you have the necessary user permissions .
53	Invalid credentials (authentication).	Get a certificate and an API key again.
101	Invalid object reputation (local reputation database).	Make sure that the value of the object reputation parameter (<code>reputation</code>) is correct. Possible values: • 1 – trusted; • 2 – untrusted.
151	Short URL (URL Reputation).	Be sure that the URL complies with RFC 3986. Enter a URL like <code>example.com</code>
152	Invalid URL (URL Reputation).	Be sure that the URL complies with RFC 3986. Enter a URL like <code>example.com</code>
153	URL address could not be processed (URL Reputation).	Be sure that the URL complies with RFC 3986. Enter a URL like <code>example.com</code>
201	Invalid file hash (File Reputation).	Be sure that the file hash is entered correctly. Kaspersky Private Security Network supports MD5 and SHA256 hash types.
202	File hash is empty (File Reputation).	Enter the file hash (<code>hash</code>). Kaspersky Private Security Network supports MD5 and SHA256 hash types.
203	The file hash does not match the stated hash type (File Reputation).	Be sure that the hash type (<code>hash_type</code>) is correctly specified.
204	Unknown hash type (File Reputation).	Be sure that the hash type parameter (<code>hash_type</code>) has the value MD5 or SHA256. Kaspersky Private Security Network does not support other hash types.
255	Unknown error (general).	Contact the Technical Support Service.
401	The client certificate is not provided or is invalid (authentication).	Get a certificate and an API key again.

Kaspersky Private Security Network log

The Kaspersky Private Security Network log is intended for diagnosing and resolving problems of the application. The Kaspersky Private Security Network log records information about events that occurred during operation of Kaspersky Private Security Network.

Kaspersky Private Security Network does not send data outside the local corporate network. Instead, it keeps the data inside the local network. The Kaspersky Private Security Network log is stored on the server on which the server part of Kaspersky Private Security Network is installed. It is impossible to totally disable the logging of information in the Kaspersky Private Security Network log, except for logging of queries for the URL Reputation and File Reputation services.

The Kaspersky Private Security Network log records the following data:

- System information about the operation of Kaspersky Private Security Network services (for example, server status, service status, information about the last update).
- IP addresses of computers of Kaspersky applications users from which the request to Kaspersky Private Security Network was made.
- Information about the operation of File Anti-Virus:
 - Hash of scanned files.
 - Hash of certificates of scanned files.
- Information about users' network activity:
 - URLs of visited websites.
 - IP addresses of visited resources.
 - Names of visited hosts.

User credentials (user name and password) are not written to the Kaspersky Private Security Network log.

- Information about inbound email:
 - IP addresses of senders of email messages.
 - Hash files in email message attachments.
 - URLs contained in email messages.
- System information about the operation of Kaspersky applications:
 - ID of the computer on which the Kaspersky application is installed.
 - User ID of the Kaspersky application.
 - Names of detected threats.

- Queries for the URL Reputation and File Reputation services.

[You can enable or disable request logging for URL Reputation and File Reputation services.](#)

The Kaspersky Private Security Network log stores data for the last 15 days.

Log archive size is capped at 10 GB. When that size cap is reached, upon adding new log records to the archive the earlier records will be deleted.

Enabling or disabling request logging for URL Reputation and File Reputation services

To enable or disable request logging for URL Reputation and File Reputation services:

1. In the web interface of Kaspersky Security Center Web Console 14.2, go to the **Operations** → **KPSN settings** section.

In the web interface of Kaspersky Security Center Web Console of a different version, go to the **Applications and services** → **KPSN** → **Settings** section.

2. On the **Configuration** tab, in the **KPSN configuration** section, select the **File Reputation** or **URL Reputation** component.
3. This opens a window with information about the component; in that window, do one of the following:
 - If you want to enable request logging, turn on the **Enable request logging** toggle switch.
 - If you want to disable request logging, turn off the **Enable request logging** toggle switch.
4. Click **Save**.

Request logging is enabled or disabled for the URL Reputation or File Reputation service.

Contacting the Technical Support Service

This section describes the ways to get technical support and the terms on which it is available.

How to get technical support

If you cannot find a solution to your problem in the documentation or other sources of information about Kaspersky Private Security Network, we recommend contacting Technical Support. Technical Support will answer your questions about installing and using Kaspersky Private Security Network.

Kaspersky provides support for Kaspersky Private Security Network throughout its life cycle (see the [Application lifecycle](#) page). Before contacting Technical Support, please read the [support rules](#).

You can contact Technical Support in one of the following ways:

- [Visit the Technical Support website](#)
- By sending a request to Kaspersky Technical Support via the [Kaspersky CompanyAccount portal](#).

Technical support via Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) is a portal for organizations that use Kaspersky applications. The Kaspersky CompanyAccount portal exists to allow users to interact with Kaspersky experts using electronic requests. On the Kaspersky CompanyAccount portal, you can monitor the processing status of electronic requests by Kaspersky experts and keep a history of electronic requests.

You can register all employees of your organization under a single Kaspersky CompanyAccount account. A single account allows you to centrally manage electronic requests from registered employees to Kaspersky, as well as manage the permissions of these employees in Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian

- French
- Japanese

You can learn more about Kaspersky CompanyAccount on the [Technical Support website](#) [↗].

Appendix

This section contains information that supplements the main text of the document.

List of ports used by Kaspersky Private Security Network

Listed below are the ports that must be opened on servers on which you want to install the server part of Kaspersky Private Security Network.

Ports required by Kaspersky Private Security Network

Connection initiator	Connection destination	Port	Protocol	Description
Kaspersky Security Center Web Console web plug-in	Kaspersky Private Security Network server	443	HTTPS	Managing Kaspersky Private Security Network
REST API client	Kaspersky Private Security Network server	80	HTTPS	Using the KPSN REST API
REST API client	Kaspersky Private Security Network server	443	HTTPS	Using the KPSN REST API
Kaspersky application	Kaspersky Private Security Network server	1443	KSN	Application requests to Kaspersky Private Security Network services
Kaspersky Private Security Network servers	The Kubernetes control node on which Kaspersky Private Security Network was installed	31000	TCP	Access to the local container repository for Kaspersky Private Security Network component deployment. Access to the external address of the Kubernetes control node is not required. For each server, access to the specified port on the same server (localhost) is sufficient. The internal Kubernetes network is also used for communication with the local repository (see below).
KPSN servers (addresses on the internal network of Kubernetes)	KPSN servers (addresses on the internal network of Kubernetes)	Any	Any	Interaction of Kaspersky Private Security Network components within the Kubernetes cluster. The networks being used depend on the configuration of Kubernetes. Default settings: 10.42.0.0/16, 10.43.0.0/16. For details, please refer to the k3s documentation.
Kaspersky Private Security Network servers	The Kubernetes control node on which Kaspersky Private Security Network was installed	6443	TCP	Interaction of Kaspersky Private Security Network components with k3s
Kaspersky Private Security Network servers	Kaspersky Private Security Network servers	8472	UDP	Interaction of Kaspersky Private Security Network components with k3s. The port is specified for the case of Flannel VXLAN being used in Kubernetes. For details, please refer to the k3s documentation.

To be able to get database updates and request configuration files, allow outgoing connections to ksn-pub-5.kaspersky-labs.com on port 443 for the following servers:

- For all servers with application components, if you are using the standard configuration of Kaspersky Private Security Network.
- For the server with the Gateway External component, if you are using Kaspersky Private Security Network with a unidirectional gateway.

List of website categories of the URL Reputation service

Verification of the reputation of websites by sending an HTTP request to the URL Reputation service also includes the identification of website categories. If the website category ID is missing from the list, this category is unknown for the current version of Kaspersky Private Security Network. The list of categories will be updated in the documentation for the next version of Kaspersky Private Security Network. Below is a list of identifiers and website categories.

List of website categories covered by the URL Reputation service

ID	Website category	Category description
0	Category not assigned	
1	Adult content	This category includes the following types of materials: • Web pages containing any photo, video or text materials depicting genitals of humans or humanoids, or acts of sexual intercourse or self-stimulation, performed by human beings or humanoids. • Web pages containing erotic materials, works that realistically portray human sexual behavior, or works of art designed to stimulate sexual arousal. • Web pages devoted to the discussion of sexuality in human relations. Web pages devoted to any sexual practice. • Web pages devoted to nudism, including but not limited to community sites, special recreation areas, and hosting of photos related to nudism. • Web pages about sex education. • Web pages providing online or offline sexual services, dating for sex, including virtual sex. • Web pages that advertise or sell items for use in sex and/or stimulation of sexual arousal. • Web pages containing information about abortion. See also Exclusions below the table.
3	Alcohol, tobacco, drugs	This category includes web resources whose content is directly or indirectly related to alcoholic or alcohol-containing products, tobacco products, electronic cigarettes, and narcotic, psychotropic and/or intoxicating substances. See also Exclusions below the table.
4	Violence	This category includes the following types of materials: • Web pages that contain any photo, video, or text content that describes or depicts physical or psychological abuse of human beings or cruelty towards animals. • Web pages that contain descriptions or depictions of murder, fights, torture, rape, or abusive actions towards human beings, animals, or imaginary creatures. • Web pages that contain descriptions or depictions of victims or atrocities of wars, armed conflicts, and other depictions of suffering people. • Web pages that contain disturbing or upsetting content, such as gore, mutilation, brutal accidents, etc. • Web pages that promote actions that constitute a threat to life and/or health, self-harm or suicide. • Web pages that contain information about eating disorders, promote them or contain approving discussions of them. • Websites associated with internationally recognized terrorist, extremist or racist organizations. See also Exclusions below the table.
5	Profanity, obscenity	This category includes web pages where profane language is detected.

6	Weapons, explosives, pyrotechnics	This category includes web resources with information about the military, weapons, explosives, and pyrotechnical products. The term "weapons" means devices, items designed to harm the life or health of humans and animals and/or damage equipment and structures. It includes replica weapons. This category includes the following types of materials: • Websites of weapons, explosives, pyrotechnical products and related accessory manufacturers and stores. • Web pages devoted to the manufacture or use of weapons, explosives, and pyrotechnical products and related accessories. • Web pages containing hunting and survival supplies (E.g. knives, survival kits, stabbing weapons, daggers...) • Web pages about shooting sports and airsoft weapons. • Web pages containing analytical, historical and manufacturing materials devoted to weapons, explosives and pyrotechnical products. • Web pages containing military-related topics, tactical gear, descriptions of armed forces, military contractors, armed conflicts, armed groups and military doctrines. See also Exclusions below the table.
8	Chats, forums, IM	This category includes web resources intended for public discussion of various topics using special web applications, as well as web resources designed to distribute or support instant messaging applications that enable real-time communication.
9	Web-based mail	This category includes login pages of email services and mailbox pages containing emails and associated data (such as personal contacts). This category does not include the other web pages of an Internet service provider that also offers email service. Any content inside the webmails is excluded from other categories (I.e. the content of emails is not categorized).
10	Online stores	This subcategory includes online shops and auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.
11	Social networks	This category includes web resources designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registration of a user account as a condition of participation.
12	Job search	This category includes web resources designed to bring together employers and job seekers: • Websites of recruitment agencies (employment agencies and/or headhunting agencies). • Websites of employers with descriptions of available job openings and their benefits. • Independent portals with employment offers from employers and recruitment agencies, including freelance platforms and job marketplaces. • Professional social networks that, among other things, make it possible to publish or find information about specialists who are not actively searching for employment. See also Exclusions below the table.
13	Anonymizers	This category includes web resources that provide information or tools to download the content of other web resources in order to: • Anonymously access web resources, including web resources that specifically reject HTTP requests from certain IP addresses or address groups (for example, IP addresses grouped by country of origin). • Bypass restrictions imposed by an internet service provider or local network administrator on access to web addresses or IP addresses. • Substitution of IP address. • Send anonymous emails. This category includes both web resources with content intended for the aforementioned purposes (VPNs, "anonymizers", etc.) as well as web resources with technically similar functionality.
14	Payment systems	This category includes web resources of e-money systems that provide access to the user's personal account. In technical terms, payment can be made using both bank cards of any type (plastic or virtual, debit or credit, local or international) and e-money. Web resources can fall into this category regardless of whether they offer technical features such as data transmission over the SSL protocol, the use of 3D Secure authentication, etc.
21	Forbidden by Police of Japan	Web resources prohibited by the Japanese police.
22	Software, audio, video	This category includes web resources where users can download software packages.
23	Finance, economics	This category includes websites that provide information about finance and economy, including but not limited to investments, taxation, accounting, insurance, brokerage activities, personal finance, retirement, mortgages and loans. This category also includes fundraising and debt collection agencies.
24	Business	This category includes websites of firms, business associations, industry groups, and corporate websites. It also includes websites that offers corporate and business-oriented services.

25	Computers, electronics	This category includes websites with content related to tech and consumer electronics: • Websites that contain information on computers, computer parts and accessories. • Websites that contain information on consumer electronics, including but not limited to tech gadgets, cell phones, televisions, home theaters, sound systems, DVD players, video game consoles, digital cameras and camcoders, printers, car electronics, and smart home devices connected to the internet. • Websites that contain tech news, how-tos and reviews of consumer electronics. • Websites of manufacturers and purveyors of the electronic devices described above and technology in general.
26	Information security	This category includes websites that contain information on IT security, including websites that provide security products and services for corporate and home users. This category does not include pages that provide information on how to hack systems. Web pages falling in this category may not be assigned to other categories.
27	Gambling, lotteries, sweepstakes	This category includes web pages offering: • Gambling in which participants can participate financially, even if such financial participation is not a mandatory condition for accessing the website. • Sweepstakes that involve betting with money. • Lotteries that involve purchasing lottery tickets or numbers. • Information that can trigger the desire to participate in gambling, sweepstakes, and lotteries. • Online games that offer free participation in a separate mode. This category may include web pages that actively advertise third party resources falling into this category. See also Exclusions below the table.
28	Internet communication	This category includes web resources that enable users (whether registered or not) to send personal messages to other users and/or post messages (either open to the public or to a limited audience) on the website.
29	Spam sites	This category includes websites specifically built for spamming and/or websites used in spam emails.
30	Transportation	This category includes websites dedicated to motor vehicles: • Websites with information, discussions and reviews of cars, motorcycles, trucks, boats, planes and trains. • Websites for shopping for new and used motor vehicles, including parts and accessories. • Websites with information about vehicle modification, repair and customization. • Websites of public transportation
31	Arts	This category includes websites that contain information about and promote visual arts, performing arts and cultural heritage: • Websites of museums, galleries and exhibitions. • Web pages that contain descriptions or depictions of visual arts, including but not limited to paintings, sculpture, architecture, literature, photography and design. • Web pages that contain descriptions or depictions of performance arts, including but not limited to theatre, dance and music. Web pages falling in this category may not be assigned to other categories.
32	Cryptocurrencies, mining	This category includes web resources offering services for buying, selling and storing cryptocurrency, as well as informational services related to cryptocurrencies and cryptomining.
33	Forbidden by laws of Belgium	Web resources blocked by the Belgian Gaming Commission.
34	Online stores, banks, payment systems	This category includes websites of online stores, payment systems, banks, online wallets and cryptocurrency websites.
35	Videogames	This category includes web pages devoted to various genre of video games: • Websites of developers whose main business is video games. • Web pages devoted to a discussion of video games. • Web pages providing the technical ability to participate in online gaming, individually or together with other players. • Web pages that allow game play with or without local installation of applications ("browser games"). • Web pages designed to advertise, distribute, and support gaming software.

36	Religions, religious associations	This category includes web pages with materials on public movements, associations, and organizations with any manifestation of a religious and/or cultlike ideology: • Websites of official religious organizations at different levels, from international religions to local religious communities. • Websites of unregistered religious associations and societies that historically emerged by splintering from a dominant religious association or community. • Websites of religious associations and communities that have emerged independently of traditional religious movements, including at the initiative of a specific founder. • Websites of inter-confessional organizations pursuing cooperation among members of different traditional religions. • Web pages with detailed portrayals or descriptions of worship in religious cults, including rites and rituals involving the worship of God, beings and/or items believed to have supernatural powers. See also Exclusions below the table.
37	News media	This category includes web resources with public news content created by mass media or online publications that let users add their own news reports: • Websites of official media outlets. • Websites offering information services with the attribution of official information sources. • Websites offering services that aggregate news or offer news from various official and unofficial sources. • Websites where news content is created by users themselves ("social news sites"). Web pages falling in this category may not be assigned to other categories.
38	Pornography, erotic	This category includes: • Web pages that contain any photos or videos depicting the genitalia of humans or humanoids, as well as intercourse or self-pleasure involving humans or humanoids. • Webpages that contain any text, including of literary or artistic text, describing the genitalia of humans or humanoids, or intercourse or self-pleasure involving humans or humanoids. • This category may also include web pages containing erotic materials or works that portray human sexuality in an arousing way, such as artwork intended to cause sexual arousal.
39	Nudism	This category includes web pages dedicated to nudism, including but not limited to nudists community websites, special recreation areas, and hosting of photos related to nudism. Websites containing such photos are included as well.
40	Lingerie	This category includes websites of lingerie manufacturers, websites selling lingerie and exhibition/fashion web pages with description of lingerie or hosting photo collections of people in lingerie.
41	Sex education	This category includes Web pages dedicated to the topic of sex education not intended to sexual arousing, including but not limited the following types of materials: • Human sexuality, sexual relationship • Sexual anatomy of humans or animals • Sexual activity • Sexual reproduction • Sexual health, safe sex tips
42	Adult dating	This category includes websites that provide online and offline dating services for an audience over 18 years of age, whose purpose is to find a sex partner. The category also includes websites that provide sexual escort services. The category may include dating services where user profiles are of a sexual or erotic nature.
43	LGBT+	This category includes websites dedicated to LGBTQ+ topics.
44	Sex shops	This category includes websites of erotic and sex goods stores and manufacturers, including such products as condoms, potency enhancers, sex accessories, video products of erotic content on physical media.
45	Drugs	This category includes the following types of materials: • Web pages containing information or a description of narcotic, psychotropic, and/or intoxicating substances. • Web pages with instructions on how to consume or produce such substances. • Web pages with information about effects of drug consumption. • This category may include websites of non-medical organizations that help drug addicts.
46	Alcohol	This category includes: • Web pages containing information about alcoholic products or a description of how to produce or consume them. • Web pages that advertise or sell alcoholic or alcohol-containing products. • Websites of alcoholic beverage manufacturers such as wineries, breweries, distilleries, etc.

47	Tobacco	This category includes: • Web pages containing information about tobacco products, e-cigarettes and accessories. • Web pages that describe how to use or consume such products. • Web pages that advertise and sell tobacco substances and paraphernalia for consuming tobacco substances.
48	Culture, society	This category includes many aspects of society and human life, including: • Religion, religious associations • Government, politics, laws • Home and family • News media • Military • Weapons • Job search • Restaurants, cafes, food • Astrology, paranormal phenomena
49	Government, politics, laws	This category includes web pages of law enforcement and government institutions at any level, independent administrative authorities, political associations and movements, law offices, legal consultation sites, and descriptions of laws. Web pages falling in this category may not be assigned to other categories.
50	Home, family	This category includes web pages that describe or advise on family lifestyle and housekeeping. Also, DIY (do it yourself) related websites, house renovation and pages about home furnishing and decoration included.
51	Military	This category includes military-related web pages. Descriptions of armed forces, military contractors, armed groups, military doctrines and militaria. Sites or discussions encouraging or discussing armed conflict. See also Exclusions below the table.
52	Restaurants, cafés, food	This category includes: • Web pages of restaurants and cafés • Websites of recipes and descriptions of food preparation techniques, including culinary communities. • Websites of grocery stores (online and offline).
53	Astrology, esoterica	This category includes web pages with content classified as mystical or esoteric: horoscopes, fortune-telling, palm reading, and magic. This category also includes research and discussions related to UFOs, extrasensory perception, and paranormal phenomena.
54	Torrents	This category includes web torrent resources distributes Peer-to-peer file sharing services, including any web pages that distributes torrent files.
55	File sharing	This category includes file sharing websites and services specifically designed to store, synchronize and share user files.
56	Audio, video	This category includes web resources distributing audio and video materials, including but not limited to movies, recordings of sports broadcasts, recordings of concerts, songs, movie clips, videos, audiovisual tutorials, etc.
57	Information technologies	This category includes many aspects of IT services and tech equipment, including: • Anonymizers • Search engines and services • Hosting, domains • Ad networks • Internet services • Computers, electronics • Information security • Spam sites
58	Search engines and services	This category includes websites that provide database of internet resources with a built-in search engine. For example: Google Search, Bing®, Yahoo! Search. Web pages falling in this category may not be assigned to other categories.
59	Hosting, domains	This category includes websites that provide hosting, domain registration, and WHOIS lookup services.
60	Ads	This category includes websites of ad agencies, ad networks. It does not block ad banner themselves.
61	Banks	This subcategory includes: • Web pages of banks offering online banking services, including wire (electronic) transfers between bank accounts, bank deposits, payments for third-party services, etc. • Websites of e-wallets that provide access to a user account.

62	Real estate	This category includes web pages for renting, selling, and buying real estate.
63	Phishing websites	This category includes web pages that contain data loss threats, including: • Phishing • Scam and other web fraud.
64	Malicious websites	Malicious software download URLs
65	Self-harm, suicide	This category includes web pages that promote actions that constitute a threat to life and/or health, self-harm or suicide.
66	Blogs	This category includes websites that powered by blog platforms, personal blog websites, and websites that provide paid or free services for creating and maintaining blogs.
67	Dating sites	This category includes websites that provide online and offline dating services.
68	Education	This category includes education-related websites.
69	Schools, universities	This category includes web pages of schools, universities, and other educational organizations. This subcategory also includes online classes and other educational web services. Web pages falling in this category may not be assigned to other categories.
70	Books, writers	This category includes writers' web pages, pages about books, and discussion sites. Fan clubs of particular authors and books. Publisher sites. Online libraries and bookstores.
71	Education portals, knowledge bases	This category includes online learning services and educational portals on various topics. Encyclopedias written by vetted experts or by users. Web pages falling in this category may not be assigned to other categories.
72	Hobbies, entertainment	This category includes web pages about different hobbies or forms of recreation. This category also includes travel, music, and pets, as well as sites related to entertainment and infotainment, including but not limited to films, the box office, theatre, television, show business, music, fan clubs, celebrity news, gossip and comics.
73	Fishing, hunting	This category includes web pages related to hunting and fishing: • Communities and forums where hunting and fishing are discussed • Websites with advice and instructions on hunting and fishing • Stores that sell fishing and hunting gear and/or weapons
74	Traveling, trips	This category includes travel-related sites: • Guides and navigation for particular countries/cities • Services for reserving hotels and tickets; reviews of hotels and resorts, travel booking services • Travel agencies that assist with reserving hotels and tickets for various forms of transportation • Online communities for discussing different types of tourism
75	TV, radio	This category includes web pages for TV companies, online TV, and websites of radio companies and online radio broadcasters.
76	Pets, animals	This category includes web pages dedicated to animals; communities and organizations dedicated to animals. This category also includes instructions on animal care and online broadcasts about animals.
77	Humor	This category includes entertainment-oriented web pages that contain jokes, memes, humorous stories, or funny videos. Sites of comedy programs and shows may be included as well.
78	Music	This category includes: • Web pages that contain song lyrics and notes • Official pages of musical groups, composers, and performers that contain songs and biographies. • Ticketing platforms for music concerts. • Sites of musical establishments: opera houses, philharmonic orchestras, etc. • This category also includes music streaming platforms and musical TV, radio channels.
79	Health, beauty, sports	This category includes web pages about sports, beauty, and health.
80	Sports, sport games	This category includes web pages about any type of sports, sports history, or game rules. This subcategory also includes sport communities, teams, athletics, fans, and sports news sites.
81	Health	This category includes web pages on healthy lifestyles. This subcategory may include sites dedicated to fitness, healthy eating, and alternative therapeutic practices and methods.
82	Fashion, style	This category includes web pages related to fashion and style: modeling agencies, fashion shows and broadcasts, and sites about fashion and style for clothing and footwear. Fashion and style guides.

83	Medicine, pharmacy	This category includes: • Web pages about medicine and pharmacies in general. • Websites of medical organization and rehabilitation centers. • Pharmaceutical companies and pages about medications and supplements. • Web pages with official information about infection preventions, including HIV and cancer prevention recommendations. • Professional medical psychological aid center. Web pages falling in this category may not be assigned to other categories.
84	Lotteries	Web pages for online lotteries and sites that contain information about lotteries.
85	Casino, card games	This category includes: • Websites of online and offline casinos. • Websites about card games and for playing gambling card games. • Websites with gambling instructions and tips. • Websites of casino producers/professional equipment and information about it.
86	Online sweepstakes	This category includes websites of online and offline bookmakers for placing bets on sports-related events, horse and other races and/or bet on other events.
87	Hate, discrimination	This category includes web pages that incite hatred toward groups of people, encourage discrimination of any kind, advocate racism and extremism, or promote self-harm or suicide.
88	Extremism, racism	This category includes the following types of materials: • Web pages promoting extremism and terrorism • Websites about terrorist and extremist organizations which are universally recognized • Web pages promoting racism and discrimination against people because of different ethnicity, beliefs or gender.
89	Other	This category is reserved for future use. You can ignore this category.
90	Anorexia	This category includes web pages that contain information about eating disorders, promote them or contain approving discussions of them. See also Exclusions below the table.
91	Abortion	This category includes web pages that contain information about abortion in general. It may include information from medical authorities.
92	Kids internet	This category includes web pages for designed for children: educational, entertainment, communication platforms. Web pages falling in this category may not be assigned to other categories.
93	Internet services	This category includes the following topics: • Main pages of global and local ISPs. • Online translators. • Website statistics and analytics services. • Internet hosting for software development. • Websites that provide web services, including but not limited to companies that provide and support networking equipment, virtualization, operative software and systems, automation tools, etc. Web pages falling in this category may not be assigned to other categories.
94	Forbidden by Russian Federation laws	Web resources blocked by legislation in the Russian Federation.
95	Russian Federal Law N 436-FZ	This category covers several categories of web resources, as described in Article 5 of Federal Law 436-FZ.
96	Current Russian Federal list of extremist materials	Web resources included in the federal list of extremist materials of the Ministry of Justice of the Russian Federation.
97	List of the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor)	Web resources included in Roskomnadzor's unified register of prohibited Internet resources.
98	Forbidden by regional laws	This category includes web resources blocked by legislation in individual countries.
99	Indecent content	This category includes web pages that provide sexually explicit text, media, services or discussions intended for an audience over 18 years of age. Such material is mostly presented in an explicit erotic way or its primary intent is to stimulate sexual arousal.

100	Sexual scenes	This category includes web pages that provide not-explicit material about sexuality. Such material is not intended for a children audience, but can be consulted by teenagers under the supervision of an adult. As an example, it includes: • Information about sexual anatomy and sexual reproduction. • Contraceptives, fertility awareness and birth planning. • Sexual health. • Tips for better sex with partner, sexual paraphernalia and sexual enhancement products. • Abortion. • Nudity without erotic intent.
113	Adware	Web pages with content related to software that downloads or displays unwanted ads when a user is online, collects marketing data and other information without the user's knowledge, or redirects search requests to certain advertising websites.
114	Riskware	Web pages with content related to legitimate programs that can cause damage if they are exploited by malicious users (in order to delete, block, modify, or copy data, and disrupt the performance of computers or networks).
122	Tor® nodes	Resource is a Tor node.
123	Dynamic DNS	Resource is provided by a dynamic DNS service.
124	Remote administration tools	Resource hosts Remote Admin Tools software.
137	Allowed website (the company's local reputation database)	
138	Forbidden website (the company's local reputation database)	
201	Banned by the Safer Internet Association of Japan	Piracy sites prohibited by the Safer Internet Association (SIA) of Japan.
203	Generative AI tools	This category includes websites of services and tools based on artificial intelligence algorithms: • Creation of original content such as text, images, videos, music, code, and so on • Analysis of existing content such as text, video, audio, code, and so on

*The "International LGBT social movement" is designated as extremist and prohibited on the territory of the Russian Federation.

Exclusions

The category and its subcategories (if any) may not include:

- Educational websites and encyclopedias.
- Websites of government institutions at all levels.
- Websites of official media outlets and newspapers.
- Websites of scientific and medical institutions.
- Websites of schools and universities.
- Websites where children are the only intended audience.

Updating third-party software used by Kaspersky Private Security Network 4.0.3 or higher

Stable operation of Kaspersky Private Security Network is guaranteed together with the versions of third-party software used by default.
If you experience problems after updating third-party software, roll back the third-party software to the versions used by default.

The distribution kit of Kaspersky Private Security Network version 4.0.3 and later includes the `upgrade_components.sh` script and the `custom_images_versions` file.

The script lets you:

- Upgrade third-party software to custom versions: for the [standard configuration](#) and for the [configuration with a unidirectional gateway](#).
- [Roll back third-party software to versions used by Kaspersky Private Security Network by default](#).

Updating third party software

To update third-party software:

1. On the Control node of the Kubernetes cluster, unpack the `KPSN_install_<version>.tar.gz` archive.
2. Open the `custom_images_versions` file extracted from the archive for editing and change the versions of the third-party software as needed.

You can edit the repository in which the image is located and the version of the image.

3. Make sure the images of all containers specified in the `custom_images_versions` file are available. To do so, do one of the following:

- Provide internet access. In this case, the script downloads the necessary containers to the `upgrade_kpsn/images` directory.
- Add images to the local container repository used by Kaspersky Private Security Network.
- Place the images in the `upgrade_kpsn/images` directory.

The file names must have the following format: `%imageName%:%tag%.tar`.

4. Make sure the Helm charts used to install containers are available. To do so, do one of the following:

- Provide internet access.

In this case, the script downloads the necessary Helm charts to the `upgrade_kpsn/charts` directory.

- Run the `./download_external_charts.sh` script, and then copy the necessary Helm charts from the 'charts' directory to the `upgrade_kpsn/charts` directory.

The file names must have the following format: `%helm_name%-%version%.tgz`.

5. Run the script:

```
./upgrade_components.sh
```

The script updates third-party software to the versions specified in the `custom_images_versions` file.

Updating third-party software in configuration with a unidirectional gateway

To update third-party software in configuration with a unidirectional gateway

1. [Update the third-party software](#) in the open network segment.
2. On the Control node of the Kubernetes cluster in the open network segment, download the necessary container images and Helm charts. To do this, run the script:

```
./upgrade_components.sh --dump
```
3. On the Control node of the Kubernetes cluster in the categorized network segment, unpack the `KPSN_install_<version>.tar.gz` archive.
4. Copy the `upgrade_kpsn` folder along with its contents and the `custom_images_versions` file, which are located on the Control node of the Kubernetes cluster in the open network segment, to the folder with the unpacked archive on the Control node of the Kubernetes cluster in the categorized network segment.

If you are prompted to confirm the replacement of files, agree.

5. On the Control node of the Kubernetes cluster in the categorized network segment, run the script:

```
./upgrade_components.sh
```

The script updates third-party software in the categorized network segment to the versions specified in the `custom_images_versions` file.

Rolling back third-party software to versions used by Kaspersky Private Security Network by default

To roll back third-party software to versions used by Kaspersky Private Security Network 4.0.3 by default:

1. Make sure that the images of the relevant containers are located in the local container repository used by Kaspersky Private Security Network.
2. If you have removed container images from the local container repository, do one of the following:
 - Provide internet access.
In this case, the script downloads the necessary containers to the `upgrade_kpsn/images` directory.
 - Add images to the local container repository used by Kaspersky Private Security Network.

- Place the images in the `upgrade_kpsn/images` directory.

The file names must have the following format: `%imageName%:%tag%.tar`.

3. Make sure the Helm charts used to install containers are available. To do so, do one of the following:

- Provide internet access.

In this case, the script downloads the necessary Helm charts to the `upgrade_kpsn/charts` directory.

- Run the `./download_external_charts.sh` script, and then copy the necessary Helm charts from the 'charts' directory to the `upgrade_kpsn/charts` directory.

The file names must have the following format: `%helm_name%-%version%.tgz`.

4. Run the script with the `--stable` option:

```
./upgrade_components.sh --stable
```

The script rolls back third-party software to versions used by Kaspersky Private Security Network 4.0.3 by default:

For a configuration with a unidirectional gateway, follow the above instructions first in the cluster in the categorized network segment, and then in the cluster in the open network segment.

Sources of information about the application

Kaspersky Private Security Network page on the Kaspersky website

On the [Kaspersky Private Security Network page](#), you can get general information about the application, its capabilities and special considerations.

Glossary

Anti-Spam

This service provides data to Kaspersky mail server protection applications so that they can filter out unwanted messages (spam) from mail traffic.

Categorized network segment

Section of a local network from which access to the Internet or to other segments of the local network is blocked.

Cloud Information

This service provides Kaspersky applications with information about the parameters of file reputation databases. The number of dangerous, safe, and other files can be displayed in a Kaspersky application.

File Reputation

This service provides Kaspersky applications with information about dangerous and safe files and displays information about the file category (e.g., computer game). The service also provides Kaspersky applications with information on the frequency of file detections in all countries of the world and the geographic distribution of the file.

Gateway External

This component keeps the reputation databases of Kaspersky Private Security Network components updated in the configuration with a unidirectional gateway. The component receives reputation database packages from Kaspersky Security Network, verifies the integrity of the data, packages the data into files, and sends the files to the categorized network segment.

Gateway Internal

This component keeps the reputation databases of Kaspersky Private Security Network components updated in the configuration with a unidirectional gateway. The component receives data files from the Gateway External component in the open network segment, unpacks them, verifies the integrity of the data, and updates the reputation databases of Kaspersky Private Security Network components on servers in the categorized network segment.

Kaspersky categories

Predefined data categories developed by Kaspersky specialists. Categories can be updated during application database updates. A security officer cannot modify or delete these predefined categories.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the continuously updated Knowledge Base of Kaspersky which contains information about the reputation of files, web resources, and software. Use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false positives.

MD5

An MD5 (Message Digest 5) checksum is a unique identifier of a file. An MD5 checksum is computed using a 128-bit hashing algorithm and is used to check the integrity of a file. There are many applications and services designed to compute the MD5 checksums of files.

Open network segment

Section of a local network from which access to the Internet or to other segments of the local network is permitted.

Record Management

This service provides anti-virus applications with information about recalls by Kaspersky AV analysts of individual virus signatures in local databases of anti-virus applications. This service is used to quickly process changes of application reputation from "dangerous" to "safe". A record to the effect that an application should be treated as malicious is stored in the local database of the anti-virus application. If the reputation has been changed, Kaspersky Private Security Network promptly updates the record in the anti-virus application database.

Spam

Unsolicited mass email messages that frequently contain advertisements.

SSL

Protocol for data encryption in local networks and on the Internet. SSL is used in web applications to create a secure connection between a client and a server.

Traffic encryption key

A unique alphanumeric sequence. A key is used to encrypt data that is transmitted between Kaspersky Private Security Network servers and computers on which Kaspersky applications are installed. The private portion of a traffic encryption key is stored on Kaspersky Private Security Network servers. The public portion of an encryption key is signed at Kaspersky and is then copied to user computers on which Kaspersky applications are installed.

Unidirectional gateway

A device intended for unidirectional transfer of data from an open network segment to a categorized network segment.

URL Reputation

This service provides the anti-virus application with information about dangerous and safe websites. The service also displays information about the website category (e.g., Adult content).

Information about third-party code

Information about third-party code is contained in the following files:

- Information about third-party code used by the server part of Kaspersky Private Security Network is contained in the legal_notices.txt file in the /usr/local/kpsn directory on the server on which the server part is installed.
- Information about third-party code used by the Kaspersky Private Security Network web plug-in is contained in the legal_notices.txt file in the <Kaspersky Security Center Web Console installation directory>/plugins/kpsn/ directory on the server on which the Kaspersky Security Center Web Console application is installed.

Trademark notices

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

Mac is a trade mark of Apple Inc.

Ubuntu, LTS are registered trademarks of Canonical Ltd.

Google Chrome and Android are the trademarks of Google LLC.

Linux is a trademark of Linus Torvalds registered in the U.S.A. and other countries.

OpenAPI is a trademark of The Linux Foundation.

Kubernetes is a registered trademark of The Linux Foundation in the USA and other countries.

Helm is a registered trademark of The Linux Foundation in the USA and other countries.

Bing, Microsoft, Windows, and Windows Server are trademarks of the Microsoft group of companies.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the USA and other countries.

Red Hat Enterprise Linux is a trademark and/or registered trademark of Red Hat, Inc. or its subsidiaries in the United States and/or other countries.

OpenSSL is a trademark of the OpenSSL Software Foundation.