

kaspersky

Kaspersky IoT Secure Gateway 1000

© 2024 AO Kaspersky Lab

Contents

[Kaspersky IoT Secure Gateway 1000 Help](#)

[About Kaspersky IoT Secure Gateway 1000](#)

[Distribution kit](#)

[Hardware and software requirements](#)

[Standard deployment of Kaspersky IoT Secure Gateway 1000](#)

[Kaspersky IoT Secure Gateway 1000 subsystems](#)

[Security recommendations for Kaspersky IoT Secure Gateway 1000](#)

[What's new](#)

[Turning the Kraftway Rubezh-N device on and off](#)

[Connecting to the Kaspersky IoT Secure Gateway 1000 web interface](#)

[Closing and resuming a connection session with the Kaspersky IoT Secure Gateway 1000 web interface](#)

[Kaspersky IoT Secure Gateway 1000 web interface](#)

[Security objectives and constraints](#)

[Processing and storing data in Kaspersky IoT Secure Gateway 1000](#)

[Data provision](#)

[About storing Kaspersky IoT Secure Gateway 1000 logs](#)

[Licensing Kaspersky IoT Secure Gateway 1000](#)

[About Kaspersky IoT Secure Gateway 1000 operating modes](#)

[Configuring Kaspersky IoT Secure Gateway 1000](#)

[Scenario: Quick Start for administrators](#)

[Scenario: Configuring access from an external network to internal network devices](#)

[Managing accounts](#)

[About account roles](#)

[Viewing information about accounts and connection settings](#)

[Configuring connection settings](#)

[Creating a user account](#)

[Updating account credentials](#)

[Managing connection certificates](#)

[Creating certificates manually](#)

[Updating certificates](#)

[Configuring the web server](#)

[Configuring network settings](#)

[Configuring the LAN settings](#)

[Configuring masquerading](#)

[Configuring the WAN settings](#)

[Configuring cellular connection settings](#)

[Modem profiles table](#)

[Enabling and disabling a cellular connection](#)

[Creating a modem profile](#)

[Copying a modem profile](#)

[Completing an empty modem profile](#)

[Editing a modem profile](#)

[Switching to a different modem profile](#)

[Deleting a modem profile](#)

[Configuring routing](#)

[Creating a static route](#)

- [Editing a static route](#)
- [Deleting a static route](#)
- [Configuring MQTT broker settings](#)
 - [Table of MQTT broker profiles](#)
 - [Creating an MQTT broker profile](#)
 - [Copying an MQTT broker profile](#)
 - [Completing an empty MQTT broker profile](#)
 - [Modifying an MQTT broker profile](#)
 - [Switching to a different MQTT broker profile](#)
 - [Deleting an MQTT broker profile](#)
 - [Limitations when configuring an MQTT broker](#)
- [Filtering application protocol traffic](#)
- [Adding device name](#)
- [Configuring the date and time](#)
- [Configuring delivery of notifications when registering events](#)
 - [Configuring delivery of event logs to the Syslog server](#)
 - [Configuring delivery of MQTT notifications](#)
- [Configuring Kaspersky Security Center Administration Server settings](#)
 - [Creating a Kaspersky Security Center Administration Server certificate](#)
 - [Updating a Kaspersky Security Center Administration Server certificate](#)
 - [Configuring the settings for connecting to Kaspersky Security Center](#)
- [Modifying the configuration of Kaspersky IoT Secure Gateway 1000 manually.](#)
 - [APPLICATIONS object](#)
 - [MQTT/LIST/profileList object list](#)
 - [NETWORK object](#)
 - [SETTINGS object](#)
 - [Configuring industrial protocol traffic filtering](#)
- [Changing the language of the Kaspersky IoT Secure Gateway 1000 web interface](#)
- [Performing common tasks](#)
 - [Monitoring the state of Kaspersky IoT Secure Gateway 1000](#)
 - [Monitoring the state of a cellular connection](#)
 - [Monitoring Kaspersky IoT Secure Gateway 1000 audit events](#)
 - [Monitoring firewall audit events](#)
 - [About firewall audit events](#)
 - [Viewing the firewall audit log](#)
 - [Exporting the firewall audit log](#)
 - [Monitoring operating system audit events](#)
 - [About operating system audit events](#)
 - [Viewing the operating system audit log](#)
 - [Exporting the system audit log](#)
 - [Viewing events when connected to Kaspersky IoT Secure Gateway 1000 via the console port](#)
 - [Exporting the system log](#)
- [Managing apps](#)
 - [Downloading and installing apps](#)
 - [Starting and stopping apps](#)
 - [Managing application launch rules](#)
 - [Removing apps](#)
 - [Monitoring the state of apps](#)

[Self-testing and integrity control in Kaspersky IoT Secure Gateway 1000](#)

[Backing up and restoring from a backup copy](#)

[Updating Kaspersky IoT Secure Gateway 1000](#)

[Restarting Kaspersky IoT Secure Gateway 1000](#)

[Managing the system with the Kaspersky Security Center 14.2 Web Console](#)

[About the Kaspersky IoT Secure Gateway 1000 administration web plug-in](#)

[Installing the Kaspersky IoT Secure Gateway 1000 administration web plug-in](#)

[Updating the Kaspersky IoT Secure Gateway 1000 administration web plug-in](#)

[Removing the Kaspersky IoT Secure Gateway 1000 administration web plug-in](#)

[Logging in and logging out of the Kaspersky Security Center 14.2 Web Console](#)

[Adding a Kaspersky IoT Secure Gateway 1000 device to the group of managed devices of the Kaspersky Security Center 14.2 Web Console](#)

[Configuring Kaspersky IoT Secure Gateway 1000 settings through the Web Console](#)

[Configuring MQTT broker settings through the Web Console](#)

[Creating an MQTT broker profile through the Web Console](#)

[Editing an MQTT broker profile through the Web Console](#)

[Switching to another MQTT broker profile through the Web Console](#)

[Deleting an MQTT broker profile through the Web Console](#)

[Configuring internal and external network settings through the Web Console](#)

[Configuring masquerading through the Web Console](#)

[Adding a device name through the Web Console](#)

[Managing certificates through the Web Console](#)

[Configuring routing via the Web Console](#)

[Creating a static route via the Web Console](#)

[Editing a static route via the Web Console](#)

[Deleting a static route via the Web Console](#)

[Configuring Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Web Console](#)

[Enabling and disabling the Kaspersky IoT Secure Gateway 1000 cellular connection through the Web Console](#)

[Creating a modem profile for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console](#)

[Editing the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console](#)

[Deleting the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console](#)

[Configuring web server using the Web Console](#)

[Filtering application protocol traffic in Web Console](#)

[Configuring the network cluster](#)

[Configuring notifications through the Kaspersky Security Center 14.2 Web Console](#)

[Configuring push notifications to a Syslog server through the Kaspersky Security Center 14.2 Web Console](#)

[Configuring delivery of MQTT notifications through the Kaspersky Security Center 14.2 Web Console](#)

[Managing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 14.2 Web Console](#)

[Viewing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 14.2 Web Console](#)

[Configuring registration of Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 14.2 Web Console](#)

[Configuring address translation rules through the Web Console](#)

[Creating an address translation rule through the Web Console](#)

[Editing an address translation rule through the Web Console](#)

[Deleting an address translation rule through the Web Console](#)

[Kaspersky IoT Secure Gateway Network Protector application management](#)

[Configuring industrial protocol traffic filtering in Web Console](#)

[Adding an IP address to the IP address allowlist](#)
[Modifying an IP address in the IP address allowlist](#)
[Deleting an IP address from the IP address allowlist](#)
[Deleting an IP address from the IP address denylist](#)

[Managing the firewall](#)
[About Firewall rules](#)
[Procedure for processing network traffic](#)
[Creating firewall rules](#)
[Editing firewall rules](#)
[Deleting firewall rules](#)
[Updating Kaspersky IoT Secure Gateway 1000 through the Web Console](#)
[Restarting Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console](#)

[Managing Kaspersky IoT Secure Gateway 1000 apps through the Web Console](#)
[Working with applications via the Web Console](#)
[Downloading and installing applications through the Web Console](#)
[Configuring app settings through the Web Console](#)
[Starting and stopping applications via the Web Console](#)
[Managing application start rules through the Web Console](#)
[Removing applications via the Web Console](#)

[Managing app certificates](#)
[Adding application certificates](#)
[Updating application certificates](#)
[Deleting application certificates](#)

[Routing apps](#)
[Creating a route for an app](#)
[Editing a route for an app](#)
[Deleting a route for an app](#)

[Contacting Technical Support](#)
[Viewing the Kaspersky IoT Secure Gateway 1000 troubleshooting page](#)

[Additional Information](#)
[Preparing to install Kaspersky IoT Secure Gateway 1000](#)
[Installing Kaspersky IoT Secure Gateway 1000](#)
[Error connecting to the Kaspersky IoT Secure Gateway 1000 web interface](#)

[Glossary](#)
[Administration Server](#)
[Administrator certificate](#)
[Application administration plug-in](#)
[Event](#)
[Internet of Things \(IoT\)](#)
[Internet of Things \(IoT\) Secure Gateway](#)
[Kaspersky IoT Secure Gateway 1000 entity](#)
[Kaspersky Security Center 14.2 Web Console](#)
[Kaspersky Security Center administrator](#)
[KasperskyOS](#)
[KSC server certificate](#)
[Managed devices](#)
[Message Queuing Telemetry Transport \(MQTT\)](#)
[MQTT broker](#)

[MQTT-topic](#)









[SSL](#)

[TLS](#)

[UEFI protection device](#)

[Information about third-party code](#)

[Trademark notices](#)

	<p>What's new</p> <p>Find out what's new in this version of Kaspersky IoT Secure Gateway 1000.</p>		<p>Update</p> <p>How to update Kaspersky IoT Secure Gateway 1000.</p>
	<p>Hardware and software requirements</p> <p>Check the requirements for Kaspersky IoT Secure Gateway 1000 and the system components.</p>		<p>Application management</p> <p>How to download, install, start, stop, set up start rules, and uninstall applications in Kaspersky IoT Secure Gateway 1000.</p> <p>Managing application certificates in the Kaspersky Security Center 14.2 Web Console</p> <p>Managing routing between applications in Kaspersky Security Center 14.2 Web Console</p>
	<p>Getting started</p> <p>How to connect to the Kaspersky IoT Secure Gateway 1000 web interface.</p> <p>How to configure Kaspersky IoT Secure Gateway 1000 to get started</p> <p>How to configure access from the external network to internal network devices.</p> <p>How to configure general Kaspersky IoT Secure Gateway 1000 settings.</p>		<p>Main capabilities</p> <p>How to set up the masquerading function.</p> <p>How to configure address translation in Kaspersky Security Center 14.2 Web Console.</p> <p>How to configure routing.</p> <p>How to configure routing in Kaspersky Security Center 14.2 Web Console.</p> <p>Managing the firewall.</p>
	<p>Monitoring</p> <p>How to view summary information about the Kaspersky IoT Secure Gateway 1000 status.</p> <p>How to view the Kaspersky IoT Secure Gateway 1000 audit event logs.</p> <p>How to download the event log for the applications installed in Kaspersky IoT Secure Gateway 1000.</p> <p>How to view Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 14.2 Web Console.</p>		<p>Additional features</p> <p>Managing accounts in Kaspersky IoT Secure Gateway 1000</p> <p>How to view the troubleshooting page.</p> <p>How to restart Kaspersky IoT Secure Gateway 1000.</p>

About Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 (also referred to as "the system") is a cyberimmune system based on the KasperskyOS operating system with a preconfigured set of application software. Kaspersky IoT Secure Gateway 1000 is installed on the Kraftway Rubezh-N embedded computer and serves as an Internet of Things (IoT) Secure Gateway for enterprise networks.

Kaspersky IoT Secure Gateway 1000 performs the following functions:

- Receives, scans, and distributes messages of sensors and other devices transmitted over the MQTT protocol.
- Registers firewall and operating system audit events.
- Ensures device security.
- Blocks or allows traffic from device IP addresses according to the firewall rules.
- Can work as a DHCP server and network address translator (NAT).

Kaspersky IoT Secure Gateway 1000 is delivered with a predefined Kaspersky IoT Secure Gateway Network Protector, which provides firewall functionality for industrial protocols. The application can monitor and filter industrial traffic from IP addresses according to network packet analysis rules and create deny rules for certain IP addresses. Network packet analysis rules are included in the Kaspersky IoT Secure Gateway 1000 kit. The application also lets you create and apply allow rules for traffic originating with specific IP addresses.

You can manage Kaspersky IoT Secure Gateway 1000 through the [local web interface](#) or remotely by using the [web plug-in for the Kaspersky Security Center 14.2 Web Console](#).

Distribution kit

The distribution kit for Kaspersky IoT Secure Gateway 1000 includes the following files:

- Installation image for Kaspersky IoT Secure Gateway 1000. The image file has a name in the format `kisg-<network device type>-<system version number>_ru_en.tar.gz`, where `<network device type>` can be `diode` for unidirectional gateway or `router` for a network router, and `<system version number>` consists of four decimal numbers separated by dots, such as `1.2.3.4`.

Kaspersky IoT Secure Gateway 1000 is delivered with the Kaspersky IoT Secure Gateway Network Protector application pre-installed.

- Script for creating a Kaspersky IoT Secure Gateway 1000 boot image.
- Archive containing the installation image for the Kaspersky Security Center 14.2 Web Console web plug-in and signature file: `WEB_Plugin_KISG_<system version number>.zip`.
- Certificate files:
 - `TlsClientAdmin.p12`: archive containing the administrator certificate and private key.
 - `TlsClientUser.p12`: archive containing the user certificate and private key.
 - `CaCert.crt` is a root certificate used for signing the administrator certificate and user certificate.

The default certificate files can be used only when [connecting to the web interface](#) for the first time, after which the administrator has to [update the certificates](#).

- File containing third party code information (Legal Notices).
- Online Help.
- Version information (Release Notes).

Hardware and software requirements

The USB ports on the Kraftway Rubezh-N embedded computer can only be used for connecting a keyboard and mouse during [initial configuration of Kaspersky IoT Secure Gateway 1000](#) or a bootable USB drive [during installation of Kaspersky IoT Secure Gateway 1000](#). Connecting other devices to the embedded computers through USB ports is not supported.

Requirements for Kaspersky IoT Secure Gateway 1000 and the hardware platform

Kaspersky IoT Secure Gateway 1000 can be installed on a Kraftway Rubezh-N embedded computer only.

The connection to the Kaspersky IoT Secure Gateway 1000 web interface is established from the network administrator's or user's computer.

Correct operation of the system web interface is guaranteed only when using the following browsers:

- Google™ Chrome™ version 118 or later.
- Mozilla™ Firefox™ versions 118 to 123. Versions 124 and later are not supported.

Requirements for Kaspersky Security Center components

To connect to Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console, Kaspersky Security Center version 14.2 must be installed in the local network of your organization.

Kaspersky IoT Secure Gateway 1000 requires the following Kaspersky Security Center components:

- Kaspersky Security Center 14.2 Administration Server
- Kaspersky Security Center 14.2 Web Console

Kaspersky Security Center and Kaspersky Security Center 14.2 Web Console are not included in the [Kaspersky IoT Secure Gateway 1000 distribution kit](#). They must be installed separately.

For information on installing Kaspersky Security Center components, please refer to the Online Help Guide for Kaspersky Security Center.

Standard deployment of Kaspersky IoT Secure Gateway 1000

The standard Kaspersky IoT Secure Gateway 1000 deployment pattern assumes installation of the system at the boundary between network segments to provide an opportunity to define a set of traffic filtering rules. An administrator can manage the system and track its state from the internal network through the [Kaspersky IoT Secure Gateway 1000 web interface](#) and via the [Kaspersky Security Center 14.2 Web Console web plug-in](#).

The base scenarios ensure the operation of Kaspersky IoT Secure Gateway 1000 as the *unidirectional gateway* and *network router* device types.

Standard deployment pattern for the unidirectional gateway

The standard deployment pattern for Kaspersky IoT Secure Gateway 1000 as a unidirectional gateway (see the image below) assumes the following:

1. The device is a software unidirectional gateway.
2. The internal and external network stacks are divided at the process level.
3. Data transfer between the internal and external networks is possible only through the special MessageConsumer programming interface.

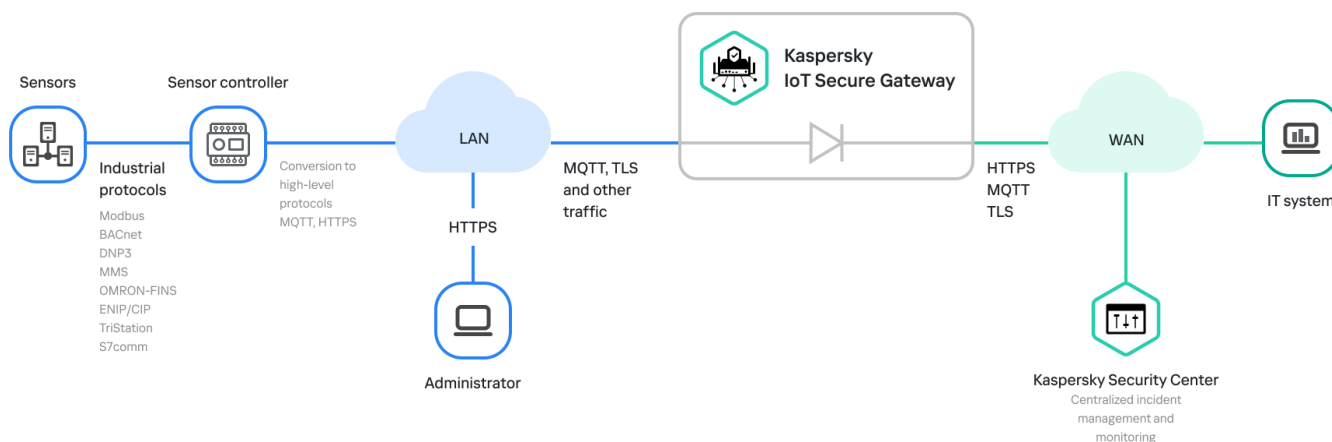
This provides unidirectional transmission of industrial telemetry data from the internal network to information systems on the external network. The TLS protocol is used to ensure the confidentiality of information being transmitted.

The MessageConsumer API is implemented in the following applications:

- Message Sender for processing traffic from the internal network
- Message Receiver for processing traffic on the external network

4. Message Sender is connected to the internal network.

5. Kaspersky IoT Secure Gateway Network Protector is connected to the internal network only.

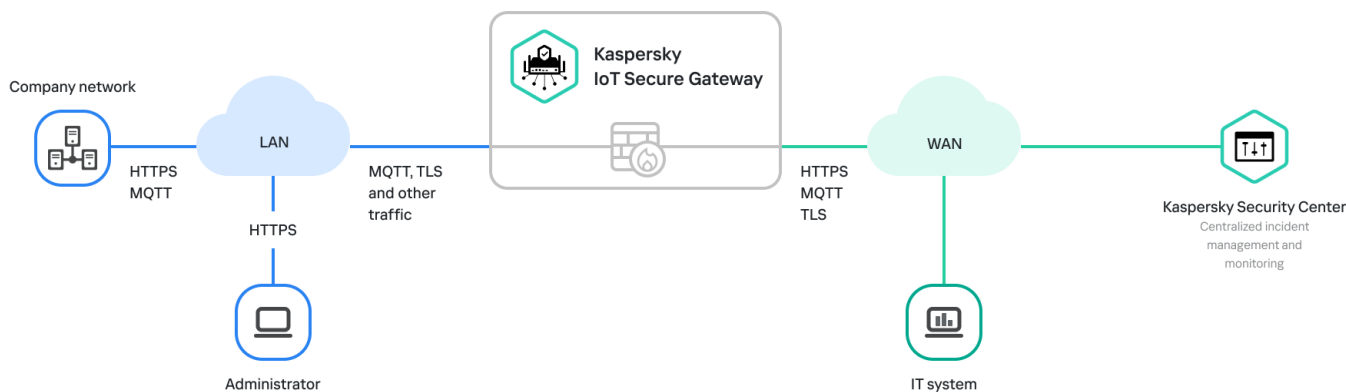


Standard deployment of Kaspersky IoT Secure Gateway 1000 as a unidirectional gateway

Standard network router deployment pattern

The standard deployment pattern for Kaspersky IoT Secure Gateway 1000 as a network router (see the image below) assumes the following:

1. The device is a network router.
2. One network stack is responsible for routing traffic between network interfaces and supports an MQTT broker (Eclipse Mosquitto™) operating on the internal and external networks for messaging.
3. Kaspersky IoT Secure Gateway Network Protector is connected to both the external and internal networks.



Standard deployment of Kaspersky IoT Secure Gateway 1000 as a network router

Kaspersky IoT Secure Gateway 1000 subsystems

Kaspersky IoT Secure Gateway 1000 includes the subsystems and entities that support its functionality. Each subsystem consists of *entities* that support individual functions of Kaspersky IoT Secure Gateway 1000.

Kaspersky IoT Secure Gateway 1000 includes the following subsystems:

- The *shared entities subsystem* includes the KasperskyOS microkernel operating system kernel, which provides minimal functionality, such as application execution scheduling, memory and I/O management, and supports and monitors communication between all system processes and entities, contains security policies, and ensures loading of dynamic libraries.
- *Drivers* support communication between the KasperskyOS operating system and hardware connectors, devices, and cards.
- The *file system* contains a set of executable files, libraries, and description files that allow using file systems and/or the network stack in a separate VFS (Virtual File System) process. A detailed VFS description is provided in the *KasperskyOS Community Edition Help*.
- *BootControl* controls Kaspersky IoT Secure Gateway 1000 boot processes.
- *WebServer* supports the [Kaspersky IoT Secure Gateway 1000 web interface](#) and [administrator and user authentication](#) functionality.
- *IdsProxy* provides communication with [Kaspersky IoT Secure Gateway Network Protector](#) and receiving notifications from it.
- *ApplicationsPlatform* provides [application management](#) including downloading, installing, and uninstalling applications, and managing certificates and permissions.

- *Notifiers* [sends Kaspersky IoT Secure Gateway 1000 events via the Message Queuing Telemetry Transport \(MQTT\) protocol and to a third-party Syslog server via the Syslog protocol.](#)
- *Troubleshooting* supports the operation of the Kaspersky IoT Secure Gateway 1000 diagnostics utilities and displays diagnostics results on the [troubleshooting page](#).
- *Kaspersky Security Center* (plug-in) supports [centralized management of Kaspersky IoT Secure Gateway 1000 through Kaspersky Security Center 14.2 Web Console](#).
- *Update* provides [updates for Kaspersky IoT Secure Gateway 1000](#), including downloading, verifying, and installing updates.
- *NetworkManagement* supports the management and operation of the [LAN and WAN](#), including the use of a cellular modem connection, a [firewall](#), and the operation of a DHCP server and DHCP client.
- *Events/Audit* [stores firewall and operating system audit events](#).
- *MQTTbroker* provides [Eclipse Mosquitto™ MQTT broker functionality](#).

This subsystem functions for the [network router device type](#) only.

- *Log* manages [Kaspersky IoT Secure Gateway 1000 logs](#).
- *SelfTesting* provides functionality for [self-testing and checking the integrity of Kaspersky IoT Secure Gateway 1000 and its entities](#), as well as [creating a backup and restoring the operating system](#).

Security recommendations for Kaspersky IoT Secure Gateway 1000

To ensure secure operation of Kaspersky IoT Secure Gateway 1000, it is recommended to restrict and control access to equipment on which the application is running.

Physical security of equipment

When deploying Kaspersky IoT Secure Gateway 1000 at a facility, you are advised to take the following measures to ensure secure operations:

- Restrict access to the room containing the hardware that has the application installed, and restrict access to the equipment of the dedicated network. Access to the room must be granted only to trusted persons, such as personnel who are authorized to install and configure the application.
- Employ technical resources or a security service to monitor physical access to equipment on which the application is running. Use security alarm equipment to monitor access to restricted rooms.
- Conduct video surveillance in restricted rooms.

Information security

For use of application management tools, it is also recommended to take the following actions to ensure data security on the intranet:

- Ensure protection of traffic within the intranet system.
- Ensure that initial configuration of Kaspersky IoT Secure Gateway 1000 is performed only within the restricted perimeter.
- Use digital certificates that were published by trusted certificate authorities. If certificates have been potentially compromised, it is recommended to update them.
- Close the connection session with the Kaspersky IoT Secure Gateway 1000 web interface when the user is finished working in the web browser. To force [termination of a connection session](#) in the web browser, you need to use the **Log out** option in the user menu.

What's new

Kaspersky IoT Secure Gateway 1000 version 3.0 has the following new capabilities and improvements:

- Edge computing: we added application support, which includes the ability to [run](#) and [manage](#) isolated applications, [manage application certificates](#), and [route data between applications](#).
Use of third-party data processing applications allows extending the functionality of Kaspersky IoT Secure Gateway 1000.
- Unidirectional gateway: Kaspersky IoT Secure Gateway 1000 can act as a unidirectional gateway-type network device for a unidirectional stream of data and commands.
- Port forwarding (destination NAT): we added an [address translation](#) feature that provides devices on the external network with access to resources on the internal network via individual ports.
- Application protocol filtering. We added firewall traffic filtering that allows [blocking network connections](#) according to the application protocol.
- Kaspersky IoT Secure Gateway Network Protector. We added an application to [monitor industrial data](#) (industrial protocol traffic analysis and filtering) including commands being transmitted.
Kaspersky IoT Secure Gateway Network Protector comes preinstalled in Kaspersky IoT Secure Gateway 1000.
- Network clustering. We added a feature that [combines multiple gateways into a fault-tolerant network configuration](#), where one of the gateways is the primary gateway and the others, a fallback option.
- Routing. We added the capability to [configure routing](#) for optimized management of network packets that traverse a device running Kaspersky IoT Secure Gateway 1000.
This functionality is available only for the *network router* device type.
- Two-factor authentication. You can now [connect to the Kaspersky IoT Secure Gateway 1000 web interface](#) in two steps: with a certificate and with credentials (name and password).
- Role-based access control. Kaspersky IoT Secure Gateway 1000 supports [two account roles](#): Administrator and User. Depending on the role, the account has access to a different set of Kaspersky IoT Secure Gateway 1000 features, settings, and data.
Kaspersky IoT Secure Gateway 1000 can contain only one Administrator account and one User account.
- Self-testing and integrity monitoring. We added the capability for [self-testing](#) of crucial subsystems to monitor the health of security functions, and the capability to [monitor the integrity](#) of system files and installed applications.
- Download applications from the Kaspersky Appcenter for Developers web portal. We added the capability to download applications uploaded to the Kaspersky Appcenter for Developers web portal and install them in Kaspersky IoT Secure Gateway 1000.
- Support for the Kraftway Rubezh-N hardware platform. Kaspersky IoT Secure Gateway 1000 can be installed on the Kraftway Rubezh-N embedded computer.
- Updating Kaspersky IoT Secure Gateway 1000. [Kaspersky IoT Secure Gateway 1000](#) is updated from Kaspersky update servers.
- Viewing the troubleshooting page. We extended the functionality around getting additional information about the way Kaspersky IoT Secure Gateway 1000 is running and [troubleshooting Kaspersky IoT Secure Gateway 1000 issues](#).

- [Audit](#) subsystem functionality has been refined and improved.
- You can now use the Kaspersky IoT Secure Gateway 1000 web interface to handle the key scenarios [for configuring and managing a device](#).
- An API for VPN client development has been added.
- Support for traffic detection and analysis (IPS) functionality has been removed. Traffic blocking functionality is provided by [Kaspersky IoT Secure Gateway Network Protector](#).
- Device discovery support has been removed.
- The [Kaspersky IoT Secure Gateway 1000 web interface](#) has been updated.

Turning the Kraftway Rubezh-N device on and off

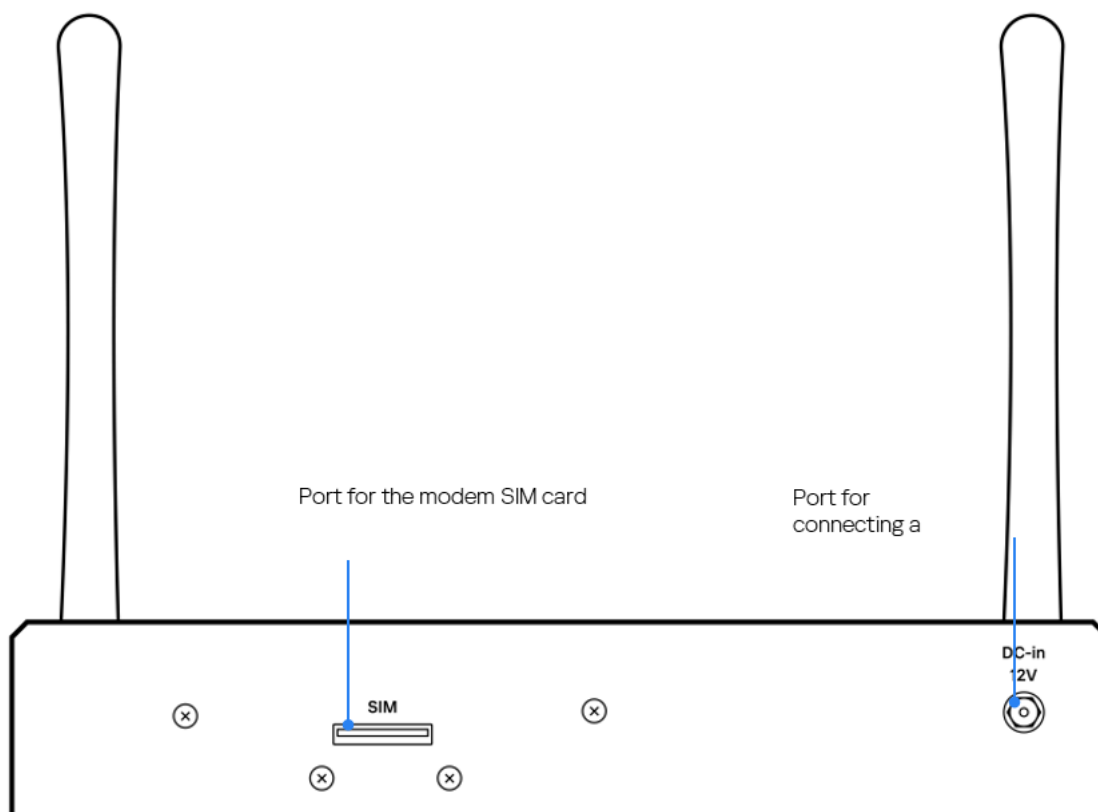
Before you start working with Kaspersky IoT Secure Gateway 1000, you must connect the Kraftway Rubezh-N device to the network and turn it on.

[Preparations for installation](#) and the actual [installation of Kaspersky IoT Secure Gateway 1000](#) are performed by Kaspersky experts.

After Kaspersky IoT Secure Gateway 1000 starts for the first time, it is recommended to [configure the network](#), [create and upload an administrator certificate](#), [configure the date and time](#), and [change the web server certificate](#) to the one that is used in your organization.

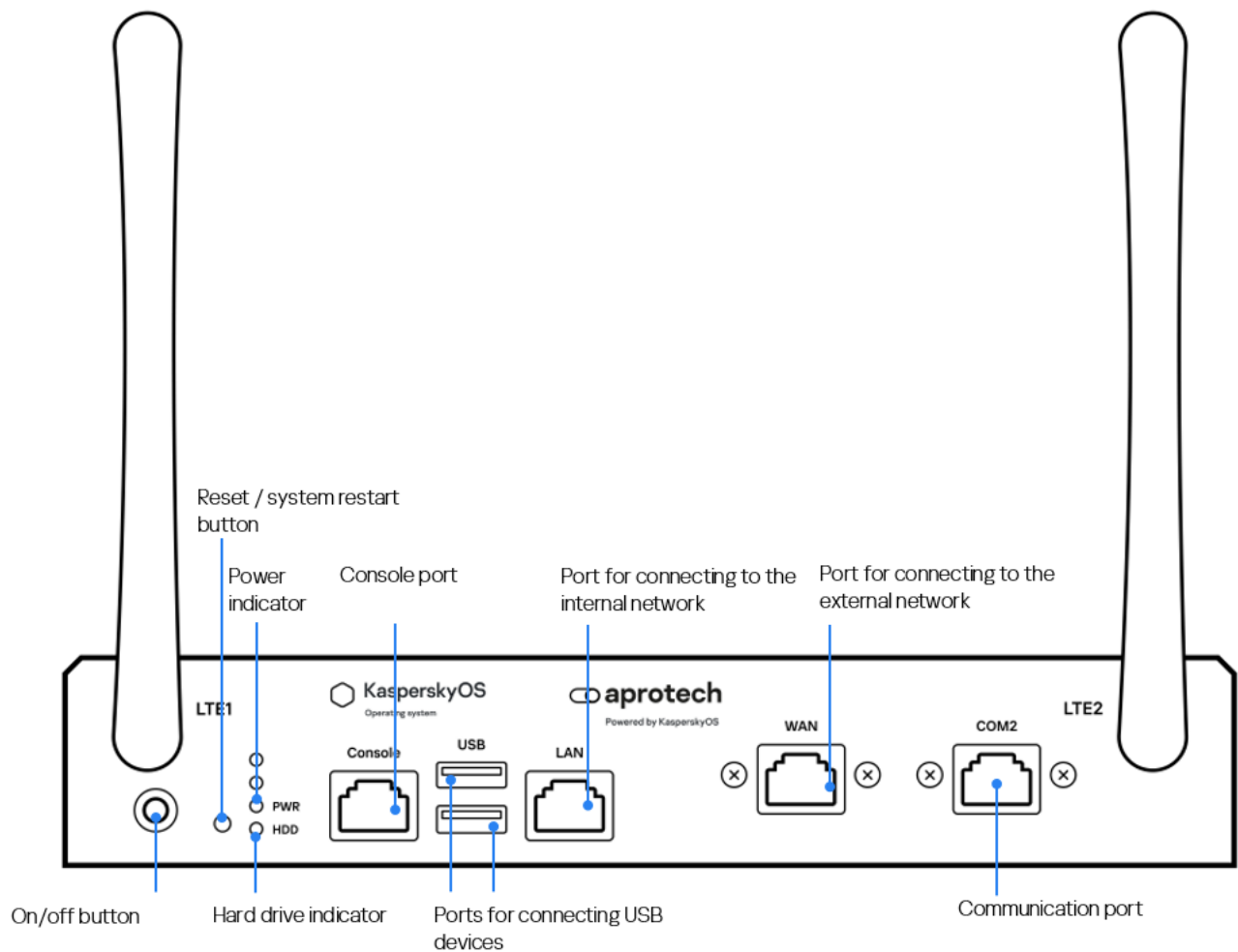
To turn on the Kraftway Rubezh-N device:

1. Connect a power cable to the port on the rear panel of the Kraftway Rubezh-N (see the figure below).



Power connector on the rear panel of the Kraftway Rubezh-N

2. Connect the external network cable to the appropriate external network port on the front panel of the Kraftway Rubezh-N (see the figure below).



Front panel of the Kraftway Rubezh-N

3. To turn on the Kraftway Rubezh-N device, press the on/off button on the left side of the front panel. The Kraftway Rubezh-N will turn on, and Kaspersky IoT Secure Gateway 1000 will start automatically.
4. To turn off the Kraftway Rubezh-N device, [close the connection session with the Kaspersky IoT Secure Gateway 1000 web interface](#) and press the on/off button on the left side of the front panel. The Kraftway Rubezh-N will turn off.

Connecting to the Kaspersky IoT Secure Gateway 1000 web interface

You can connect to the Kaspersky IoT Secure Gateway 1000 web interface using any [supported browser](#). The browser must be installed on a computer that has access to Kaspersky IoT Secure Gateway 1000 through the internal network. Kaspersky IoT Secure Gateway 1000 is delivered with a statically configured IP address of 192.168.1.1. The DHCP server is enabled by default in Kaspersky IoT Secure Gateway 1000. Therefore, when you connect your computer to the network that is connected to Kaspersky IoT Secure Gateway 1000 through its internal network connector, your computer will receive an IP address automatically.

Connection to the Kaspersky IoT Secure Gateway 1000 web interface is established using two-factor authentication, which requires the following data:

- Account name and password.

You can find the name and password of the administrator account for the *first connection* to the web interface in the instructions for the first connection provided below. These credentials are temporary and are changed by the administrator after the first login to the web interface.

- Administrator certificate or user certificate

The certificates for the administrator's *first connection* to the web interface are uploaded to Kaspersky IoT Secure Gateway 1000 by default. After the first connection, the administrator has to [update these certificates](#).

The administrator or user certificate is also used to create a secure connection between Kaspersky IoT Secure Gateway 1000 and the browser used for the connection. The archive with the certificate for the administrator's first connection to the web interface is included in the [distribution kit](#). The administrator must upload this archive to the browser before connecting to Kaspersky IoT Secure Gateway 1000 for the first time. After [renewing certificates](#), the administrator and the user must upload the new certificates to the browser.

The steps to connect to the Kaspersky IoT Secure Gateway 1000 web interface depend on your [role in the system](#) (administrator or user).

When connecting to Kaspersky IoT Secure Gateway 1000, only one active session is possible at a time. If the administrator connects to the web interface of Kaspersky IoT Secure Gateway 1000 during an active user session, the user connection session will be terminated. The user also cannot connect to the web interface of Kaspersky IoT Secure Gateway 1000 during an active administrator session.

Administrator

Before connecting to the Kaspersky IoT Secure Gateway 1000 web interface, make sure that you have a USB drive or USB token with a valid certificate.

Depending on whether you connect to the Kaspersky IoT Secure Gateway 1000 web interface for the first time or not for the first time, use one of the following approaches:

- [First connection to the Kaspersky IoT Secure Gateway 1000 web interface](#) 

To connect to the Kaspersky IoT Secure Gateway 1000 web interface for the first time:

1. Connect a USB drive with the TlsClientAdmin.p12 archive containing the administrator certificate to the computer that you want to use for connecting to the Kaspersky IoT Secure Gateway 1000 web interface.

The TlsClientAdmin.p12 archive for the first connection to the web interface is included in the [distribution kit](#).

2. Upload the certificate from the TlsClientAdmin.p12 archive to the browser. You can find information on how to upload the archive with the certificate to the browser in the browser documentation.

A password is required to upload the certificate to the browser. Default certificate password: **adminadmin**.

3. Open your browser and in the address bar, enter the IP address of Kaspersky IoT Secure Gateway 1000 web interface: <https://192.168.1.1>.

The Kaspersky IoT Secure Gateway 1000 login page opens.

4. Enter the default name and password and click **Continue**.

User name for the first login to the web interface: **admin**.

Password for the first login to the web interface: **adminadmin**.

These credentials are temporary and are required only for the first connection to the Kaspersky IoT Secure Gateway 1000 web interface. They must be changed at the next step.

5. In the credentials change window that opens, enter the new name and password and click **Save**.

The password must contain at least 8 unique characters. Your account credentials are updated, and the [Kaspersky IoT Secure Gateway 1000 web interface page](#) opens.

After you connect to the Kaspersky IoT Secure Gateway 1000 web interface for the first time, we recommend [updating the certificates](#) and [creating a user account](#).

- [Reconnection to the Kaspersky IoT Secure Gateway 1000 web interface](#) 

To connect to the Kaspersky IoT Secure Gateway 1000 web interface again:

1. If a USB token is used to access the Kaspersky IoT Secure Gateway 1000 web interface:
 - Make sure that the software supplied to support the token operation is installed on the computer from which the web interface is being accessed.
 - Make sure the token is connected to the computer from which the web interface is being accessed.
2. If the USB token *is not used*, make sure that the archive with the administrator certificate required for creating a secure connection is uploaded to the browser. You can find information on how to upload the archive with the certificate to the browser in the browser documentation.
3. Open your browser and in the address bar, enter the IP address of Kaspersky IoT Secure Gateway 1000 web interface: <https://192.168.1.1>.
4. If a USB token is used to access the Kaspersky IoT Secure Gateway 1000 web interface:
 - a. In the certificate selection window that opens, select the certificate located on the USB token and click **OK**.
 - b. Enter the token password.

If a USB token *is not used*, skip this step.

5. Enter your login and password and click **Continue**.

If you enter incorrect account information multiple times, the system is temporarily blocked (the default blocking time is five minutes). When the blocking time expires, you can try again.

If your connection is successful, the browser window displays the [Kaspersky IoT Secure Gateway 1000 web interface](#) page.

User

Before connecting to the Kaspersky IoT Secure Gateway 1000 web interface, do the following:

- Make sure you have a USB drive or USB token with a valid user certificate.
- Request your user name and password from the administrator upon the first connection or after your account credentials have expired).

You can connect to the Kaspersky IoT Secure Gateway 1000 web interface only after the administrator has [created your user account](#).

To connect to the Kaspersky IoT Secure Gateway 1000 web interface:

1. If a USB token is used to access the Kaspersky IoT Secure Gateway 1000 web interface:
 - Make sure that the software supplied to support the token operation is installed on the computer from which the web interface is being accessed.
 - Make sure the token is connected to the computer from which the web interface is being accessed.

2. If the USB token *is not used*, make sure that the archive with the user certificate required for creating a secure connection is uploaded to the browser. You can find information on how to upload the archive with the certificate to the browser in the browser documentation.
3. Open your browser and in the address bar, enter the IP address of Kaspersky IoT Secure Gateway 1000 web interface: <https://192.168.1.1>.
4. If a USB token is used to access the Kaspersky IoT Secure Gateway 1000 web interface:
 - a. In the certificate selection window that opens, select the certificate located on the USB token and click **OK**.
 - b. Enter the token password.

If a USB token *is not used*, skip this step.

5. Enter your login and password and click **Continue**.

If you enter incorrect account information multiple times, the system is temporarily blocked (the default blocking time is five minutes). When the blocking time expires, you can try again.


If your connection is successful, the browser window displays the [Kaspersky IoT Secure Gateway 1000 web interface](#) page.

Closing and resuming a connection session with the Kaspersky IoT Secure Gateway 1000 web interface

For security purposes, Kaspersky IoT Secure Gateway 1000 allows only one connection session with the web interface (in other words, if one user is connected to the web interface, others cannot connect). For this reason, it is recommended to close the connection session in the browser when you are done working with Kaspersky IoT Secure Gateway 1000 through the web interface.

If you close the browser window without first closing the connection session, the session remains active. An unclosed session remains active for 5 minutes by default. During this time, the system can grant access to the Kaspersky IoT Secure Gateway 1000 web interface without requesting a certificate and prompting for a user name and password, if the same computer and browser are used for reconnection. If necessary, the administrator can [change the duration of the unclosed session](#).

To terminate a connection session with the Kaspersky IoT Secure Gateway 1000 web interface:

1. In the left part of the page in the web interface menu, select  **<user name>**.
2. In the opened user menu, select **Log out**.

The browser window displays the Kaspersky IoT Secure Gateway 1000 login page.

For security purposes, the connection session to the Kaspersky IoT Secure Gateway 1000 web interface terminates after five minutes of system inactivity, and the login page opens. To [resume the connection session](#), you have to enter your user name and password.

Kaspersky IoT Secure Gateway 1000 web interface

Kaspersky IoT Secure Gateway 1000 is managed using a web interface. This section provides a description of the main elements of the Kaspersky IoT Secure Gateway 1000 web interface.

The main window of the web interface contains the following items:

- Menus – sections in the left part of the web interface window
- Tabs in the upper part of the web interface window for certain sections (for example, for the **Settings** section)
- Workspace in the central part of the web interface window

Sections of the web interface

The Kaspersky IoT Secure Gateway 1000 web interface menu contains the following sections:

- **Status.** In this section, you can [view summary information about the system operation](#): information about the device, the Kaspersky IoT Secure Gateway 1000 device type, and the Kaspersky Security Center connection status. This section also contains the links to the articles in the Online Help.
- **Events.** In this section, you can [view firewall audit events](#), such as events from the Kaspersky IoT Secure Gateway Network Protector application. Firewall audit events include blocking of device traffic and reconfiguring of firewall rules.

When a critical event occurs, an exclamation mark  *alarm icon* is displayed next to the **Events** menu section.

- **Audit.** In this section, you can [view operating system audit events](#). Operating system audit events include connections to the Kaspersky IoT Secure Gateway 1000 web interface, application actions, and system and component updates.

When a critical event occurs, an exclamation mark  *alarm icon* is displayed next to the **Audit** menu section.

- **Users.** This section contains the following tabs, where you can manage the user accounts and the web server settings:
 - **User settings.** On this tab, you can [view and edit account credentials](#), and [update connection certificates](#).
 - **Web server settings.** On this tab, you can [renew the web server connection certificate](#).
- **Applications.** This section contains the following tabs, where you can [manage applications](#):
 - **All apps.** On this tab, you can view information about all applications available for installation in Kaspersky IoT Secure Gateway 1000 and [install the necessary applications](#).
 - **Installed apps.** On this tab, you can manage the installed applications: [start or stop applications](#), [configure startup settings](#), and [uninstall applications](#).
 - **Application log.** On this tab, you can [download logs of the installed applications](#).
- **Network.** This section contains the following tabs, where you can configure the network settings:
 - **Internal network.** On this tab, you can view and change the [internal network settings](#).
 - **External network.** On this tab, you can view and change the settings for [network address translation](#), [external network](#), and [modem](#).

- **Routing.** On this tab, you can view and manage the [network packet routes](#).
- **Filtering.** On this tab, you can [select the protocols](#) for which you want to block the traffic.
- **MQTT broker.** On this tab, you can [view and change the settings in the MQTT broker profile](#).
- **Self-diagnostics.** In this section, you can [run the status test and the system integrity check](#), as well as view the current system status and the scan results.
- **Settings.** This section contains the following tabs where you can view and change the system settings:
 - **General.** On this tab, you can view and change the [device name](#) and the [date and time settings](#) of Kaspersky IoT Secure Gateway 1000.
 - **Notifications.** On this tab, you can view and edit the [settings for forwarding firewall and system audit logs](#) to a third-party Syslog server and configure the settings for [MQTT notifications](#).
 - **Administration Server.** On this tab, you can view and [change the settings for connecting to the Kaspersky Security Center Administration Server](#).
 - **Diagnostics.** On this tab, you can [save the Kaspersky IoT Secure Gateway 1000 system log](#) on the local computer.
 - **Configuration.** On this tab, you can view and change the [Kaspersky IoT Secure Gateway 1000 configuration settings](#).
 - **Update.** On this tab, you can update Kaspersky IoT Secure Gateway 1000.
 - **Commands.** On this tab, you can reboot the device.
 - **Backup and recovery.** On this tab, you can manage [system backup and restore from a backup copy](#): create and download a system configuration backup, as well as restore the system configuration from a previously saved backup copy.
- **About.** This section contains information about the system version installed on your device, and provides links to the Online Help Guide (direct link and QR code) and third party code information.
- **KasperskyOS.** Clicking the logo opens a window that displays the KasperskyOS (SDK) version and a link to third party code information.

Workspace of the web interface window

The workspace displays the information that you choose to view in the menus and on the tabs of the web interface window. It also contains control elements that you can use to configure how the information is displayed.

User menu

The lower-left corner of the web interface window contains a user menu that lets you do the following:

- [Change the web interface language](#).
- [Log out](#).

Security objectives and constraints

Definitions and general provisions

The goal of the cyberimmune approach to development is to create a *cyberimmune system*: a system whose declared assets are protected against undesirable events under any conditions, even under attack, subject to predefined constraints.

One prerequisite when developing a cyberimmune system is to identify its security objectives and the security constraints under which the system will operate.

Security objectives are the particular requirements imposed on a cyberimmune information system that must be fulfilled to ensure that the system operates securely in any possible usage scenario with consideration of the necessary security constraints.

Security constraints are the additional restrictions placed upon the system operating conditions that either simplify or complicate the fulfillment of security objectives.

Application is a component installed on top of the system image and started by means of Kaspersky IoT Secure Gateway 1000. May be developed by Kaspersky or supplied by a partner. The application communicates with Kaspersky IoT Secure Gateway 1000 and other applications through an API provided by Kaspersky IoT Secure Gateway 1000.

Application package is a set of all files that make up an application.

Application image is a set of executable files and libraries that make up an application.

Audit event is a security event, such as a reboot, system version update, or information security event.

Hardware platform is a target device on which the system image is installed.

Data and information are any information in digital form, such as application files or data stored in databases.

Kaspersky IoT Secure Gateway 1000 network device types:

Kaspersky IoT Secure Gateway 1000 can operate as one of the following types of network device:

- *Network router* is a type of network device that applies a policy to route traffic that passes through the device.
- *Unidirectional gateway* is a type of network device that applies a policy to ensure that devices on the LAN transmit data to the WAN, whereas local resources are not exposed to any impact from the WAN.

The network device switches between the types while running. For the changes to take effect, a full reinstallation of Kaspersky IoT Secure Gateway 1000 is required.

Kaspersky IoT Secure Gateway 1000 security objectives:

Kaspersky IoT Secure Gateway 1000 has the following security objectives:

- Kaspersky IoT Secure Gateway 1000 ensures secure (integrity and authenticity) system and application updates even when using untrusted data channels.

- Kaspersky IoT Secure Gateway 1000 ensures secure (integrity and authenticity) storage of system settings and configurations received from a trusted source. Trusted sources of information are:
 - Kaspersky Security Center Administration Server.
 - Administrator authorized by means of a certificate when installing a secure channel between the administrator's computer and Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 ensures secure (integrity) storage of audit events and transfer of these to Kaspersky Security Center Administration Server in a manner that guarantees security (integrity and authenticity).
- Kaspersky IoT Secure Gateway 1000 provides a secure (integrity and confidentiality) communication channel to the remote server (via TLS terminator).
- While running, Kaspersky IoT Secure Gateway 1000 ensures the integrity and authenticity of application packages during dynamic installation.
- Kaspersky IoT Secure Gateway 1000 ensures the integrity and authenticity of application images before these run.
- While running, Kaspersky IoT Secure Gateway 1000 enables granting of privileges to dynamically launched applications.
- Kaspersky IoT Secure Gateway 1000 ensures that Kaspersky Security System policies are applied to any communication between applications and Kaspersky IoT Secure Gateway 1000.
- Kaspersky IoT Secure Gateway 1000 provides a secure (integrity and confidentiality) dedicated data storage to each application. Only the application whose data is stored in the storage has access to it.
- Kaspersky IoT Secure Gateway 1000 guarantees communication between applications and external systems through a secure (integrity and confidentiality) communication channel (via the TLS terminator) only.
- When operating in unidirectional gateway mode, Kaspersky IoT Secure Gateway 1000 ensures unidirectional data transfer from applications interacting with the LAN to applications interacting with the WAN, while preventing local resources from being exposed to any impact originating on the WAN.

Kaspersky IoT Secure Gateway 1000 security assumptions:

The security constraints of Kaspersky IoT Secure Gateway 1000 are as follows:

- Threats associated with a vulnerability of the hardware platform are not considered. The hardware platform is assumed to be trusted.
- The device on which Kaspersky IoT Secure Gateway 1000 is installed is operating in an environment that completely eliminates the possibility of any physical access by a cybercriminal, including their inability to directly connect to the device. Threats associated with relevant vulnerabilities are out of consideration.
- A medium level of threat (basic elevated) from the external network is assumed.
- A low level of threat (basic) from the internal network is assumed.

For more information on assessing the information security threat level, please refer to the website of Federal Service for Technical and Export Control of Russia.

- Initial configuration should be done in an environment that rules out spoofing of Kaspersky Security Center Administration Server—that is, by a trusted administrator in a monitored zone.
- When operating in unidirectional gateway mode:
 - The integrity of data transmitted over the LAN from devices to the gateway is not a guarantee.
 - Devices connected to the gateway are not protected against attacks originating on the LAN.
 - The hardware platform must have separate physical ports for connecting to the LAN and WAN.
- Availability of Kaspersky IoT Secure Gateway 1000 is not a security objective.
- Security objectives are not guaranteed when installing VPN applications or Kaspersky Debug Service (KDS). When one of these applications is installed, the device restarts and exits cyberimmune mode. To return to cyberimmune mode, you have to completely reinstall Kaspersky IoT Secure Gateway 1000 and repeat the initial configuration.

Processing and storing data in Kaspersky IoT Secure Gateway 1000

This section contains information about data provision and the logs used for storing data.

Data provision

Kaspersky IoT Secure Gateway 1000 does not transmit the personal data of users to Kaspersky. Personal data of users is not processed on Kaspersky IoT Secure Gateway 1000 devices.

The operating system audit event log, firewall audit event log, system log, and application logs are not deleted when Kaspersky IoT Secure Gateway 1000 starts. All certificate details are stored in a separately allocated space on the drive.

When deleting information or files automatically or manually, a special erasure method is used, in which the deleted objects of the file system are overwritten twice with special bit sequences. For example, this method is used for deleting the administrator certificate and user certificate when they are updated.

When working with Kaspersky IoT Secure Gateway 1000, the following information is stored in cookie files:

- ID of the current connection.
- Last selected language of the Kaspersky IoT Secure Gateway 1000 web interface.
- Last visited section of the Kaspersky IoT Secure Gateway 1000 web interface in case the user did not terminate the connection session with Kaspersky IoT Secure Gateway 1000 or closed the web interface before terminating the connection session.

When a certificate is uploaded, its data fields may save personal data of the user. You need to check the contents of these fields before uploading a certificate in the Kaspersky IoT Secure Gateway 1000 web interface.

When configuring MQTT broker settings, the contents of the configuration file may contain personal data. You need to check the data uploaded to the MQTT broker profile of Kaspersky IoT Secure Gateway 1000.

Kaspersky IoT Secure Gateway 1000 saves the following information that does not include personal data:

- Network device type
- Kaspersky Security Center Administration Server connection status.
- Firewall audit log.
- Operating system audit log.
- User accounts settings:
 - General settings:
 - Number of failed login attempts before locking

- Time to wait after a failed login
- Root certificate settings:
 - Certificate file name
 - Remaining certificate validity period
- Administrator account settings:
 - Account name
 - Credentials expiration date
 - Certificate expiration date
- User account settings:
 - Account name
 - Credentials expiration date
 - Certificate expiration date
- Kaspersky IoT Secure Gateway 1000 web server settings:
 - Web server certificate name
 - Subject name
 - Certificate issuer
 - Certificate validity period
- List of applications available to install
- List of installed applications:
 - Application name
 - Application version
 - Size
 - Application type
 - Application start rules
 - Manifest
 - Application status
 - Set of Kaspersky IoT Secure Gateway Network Protector industrial protocol filtering rules (if the application is installed)
- Application logs

- Network settings:
 - LAN settings:
 - IP address of Kaspersky IoT Secure Gateway 1000 within the internal network
 - Subnet mask.
 - MAC address
 - DHCP server settings:
 - DHCP server usage (enabled or disabled);
 - Start and end of IP address range;
 - Primary DNS server address;
 - Secondary DNS server address.
 - WAN settings:
 - Address translation (NAT) settings: masquerading status (enabled or disabled)
 - DHCP client settings:
 - DHCP client usage (enabled or disabled);
 - IP address;
 - Subnet mask;
 - Default network gateway;
 - Primary DNS server address;
 - Secondary DNS server address;
 - MAC address.
 - Cellular connection settings of Kaspersky IoT Secure Gateway 1000:
 - Modem operating status
 - Modem signal strength
 - Use of the modem as the main communication channel (enabled or disabled)
 - Modem DNS server addresses
 - Telecom carrier profile details: profile activity indicator, indicator of profile editability, profile name, profile configuration file details (file type, file name, file content)
 - Routing settings:
 - Route type

- Route IP address
- Network mask
- Gateway
- Route status
- MQTT broker settings:
 - Indicator of whether the profile can be edited
 - Indicator of whether the profile is active
 - Profile name
 - Date and time of the most recent change in the profile
 - CA certificate for the MQTT server (the certificate may be self-signed)
 - Client certificate for the MQTT server
 - Private key for the client certificate of the MQTT server
 - Information about configuration files: file name, file type, file contents
- Application protocol filtering settings:
 - List of protocols for blocking traffic:
 - FTP
 - HTTP
 - MQTT
 - Modbus
 - SMTP
 - IMAP
 - POP3
 - Traffic blocking status by protocol (blocked or allowed)
- Self-diagnostics details:
 - Integrity check information: last check date
 - Self-test details:
 - Summary self-test status
 - Test name

- Test status
- Test type
- Last test date
- Test details
- General settings of Kaspersky IoT Secure Gateway 1000:
 - Device name
 - System date and time
 - Notification settings:
 - Settings of Syslog notifications:
 - Forwarding of notifications to the Syslog server (enabled or disabled)
 - IP address and port of the Syslog server
 - Notification forwarding mode: UDP, TCP, TLS
 - Syslog server certificate
 - Settings of MQTT notifications:
 - Forwarding of notifications over the MQTT protocol (enabled or disabled)
 - MQTT server address and port
 - MQTT-topic name
 - Use of authentication when sending notifications over the MQTT protocol (enabled or disabled)
 - User name and password for authentication
 - SSL for authentication (enabled or disabled)
 - CA certificate for sending notifications over the MQTT protocol
 - Client certificate for sending MQTT notifications
 - Private key of the client certificate for sending MQTT notifications
 - Kaspersky Security Center Administration Server connection settings:
 - Kaspersky Security Center Administration Server certificate
 - Kaspersky Security Center Administration Server address and port
 - System log with diagnostic information
 - Device configuration in JSON format

- Kaspersky IoT Secure Gateway 1000 information:
 - Kaspersky IoT Secure Gateway 1000 version
 - Links to online help
 - Third party code information
- Information about KasperskyOS:
 - Operating system version
 - Third party code information

If Kaspersky IoT Secure Gateway 1000 is connected to Kaspersky Security Center, Kaspersky IoT Secure Gateway 1000 saves and processes the following information that does not include personal data:

- List of applications available to install
- List of installed applications:
 - Application name
 - Application version
 - Publication date
 - Category
 - Application status
 - Application configuration
- Installed applications settings:
 - Information about installed applications:
 - Application name
 - Application version
 - Application type
 - Application status
 - Application start rule
 - Application manifest
 - Application certificates:
 - Certification Authority certificate file name
 - Certification Authority certificate principal name
 - Certification Authority certificate issuer

- Certification Authority certificate validity period (expiry date)
- Client certificate file name
- Client certificate subject name
- Client certificate issuer
- Client certificate validity period (expiry date)
- Client certificate key file name
- Routing apps:
 - Route status
 - Source app
 - Source connection point
 - Destination app
 - Destination connection point
- MQTT broker settings:
 - Indicator of whether the profile can be edited
 - Indicator of whether the profile is active
 - Profile name
 - CA certificate for the MQTT server (the certificate may be self-signed)
 - Client certificate of the MQTT server
 - Private key for the client certificate of the MQTT server
 - Information about configuration files: file name, file type, file contents
 - Certificate for sending MQTT notifications
- Network settings of Kaspersky IoT Secure Gateway 1000:
 - LAN settings:
 - IP address of Kaspersky IoT Secure Gateway 1000 within the internal network
 - Subnet mask.
 - MAC address.
 - DHCP server settings:
 - DHCP server usage (enabled or disabled);

- Start and end of IP address range;
 - Primary DNS server address;
 - Secondary DNS server address.
- WAN settings:
 - Address translation (NAT) settings: masquerading status (enabled or disabled)
 - DHCP server settings:
 - DHCP client usage (enabled or disabled);
 - IP address;
 - Subnet mask;
 - Default network gateway;
 - Primary DNS server address;
 - Secondary DNS server address;
 - MAC address.
- Routing settings:
 - Route type
 - IP address;
 - Network mask
 - Gateway
 - Route status
- Firewall rules:
 - List of rules
 - State of a rule (enabled or disabled)
 - Action that the firewall must take on network traffic that matches a rule
 - Zone to which the rule is applied
 - IP address of the traffic source
 - Port of the traffic source, if this setting is applicable to the utilized protocol
 - IP address of the traffic destination
 - Port of the traffic destination, if this setting is applicable to the utilized protocol

- Utilized protocol
- Cellular connection settings of Kaspersky IoT Secure Gateway 1000:
 - Modem operating status
 - Modem signal strength
 - Use of the modem as the main communication channel (enabled or disabled)
 - Modem DNS server addresses
 - Telecom carrier operation details: configuration file activity indicator, indicator of configuration file editability, configuration file type, configuration file name, configuration file content
- Kaspersky IoT Secure Gateway Network Protector settings (if the application is installed):
 - Set of rules for filtering industrial protocol traffic
 - IP address denylist
 - IP address allowlist
- Application protocol filtering settings:
 - List of protocols for blocking traffic:
 - FTP
 - HTTP
 - MQTT
 - Modbus
 - SMTP
 - IMAP
 - POP3
 - Traffic blocking status by protocol (blocked or allowed)
- Network cluster settings:
 - Network cluster status (enabled or disabled)
 - Cluster device priority
 - Virtual IP address
 - Virtual IP address mask
 - Cluster identifier
- Kaspersky IoT Secure Gateway 1000 general device settings:

- Device name
- Time of last synchronization with device
- Connection certificate details:
 - Details of the administrator certificate for Kaspersky IoT Secure Gateway 1000 web interface connection:
 - Certificate file name
 - Subject name
 - Certificate issuer
 - Certificate validity period
 - Kaspersky Security Center Administration Server certificate details:
 - Certificate file name
 - Subject name
 - Certificate issuer
 - Certificate validity period
- Web server settings:
 - Web server certificate details:
 - Certificate file name
 - Subject name
 - Certificate issuer
 - Certificate validity period
 - Certificate key information: key file name
- Notification settings:
 - Settings of Syslog notifications:
 - Forwarding of notifications to the Syslog server (enabled or disabled)
 - IP address and port of the Syslog server
 - Notification forwarding mode: UDP, TCP, TLS
 - Syslog server certificate
 - Settings of MQTT notifications:
 - Forwarding of notifications over the MQTT protocol (enabled or disabled)

- MQTT server address and port
- MQTT-topic name
- Use of authentication when sending notifications over the MQTT protocol (enabled or disabled)
- User name and password for authentication
- SSL for authentication (enabled or disabled)
- CA certificate for sending MQTT notifications
- Client certificate for sending MQTT notifications
- Private key of the client certificate for sending MQTT notifications
- Settings for interaction between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console:
 - Synchronization period for synchronizing the settings of Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console
 - List of commands that the Kaspersky Security Center 14.2 Web Console can send to Kaspersky IoT Secure Gateway 1000
- Kaspersky IoT Secure Gateway 1000 version information

Any received information is protected by Kaspersky in accordance with the requirements established by law and in accordance with current regulations of Kaspersky. Data is transmitted over encrypted communication channels.

About storing Kaspersky IoT Secure Gateway 1000 logs

Kaspersky IoT Secure Gateway 1000 saves [firewall audit](#) and [system audit](#) events data in relevant logs. The contents of the logs are stored in the Kraftway Rubezh-N device memory.

Kaspersky IoT Secure Gateway 1000 saves firewall and system audit event data. You can use the Kaspersky IoT Secure Gateway 1000 web interface to save a file containing a [firewall audit event log](#) and a [system audit event log](#) to the local computer.

If required, you can also configure [forwarding of data from the firewall and system audit log](#) over the MQTT and Syslog protocols.

Licensing Kaspersky IoT Secure Gateway 1000

The terms of using the Kaspersky IoT Secure Gateway 1000 system are provided in the End User License Agreement or a similar document (for example, a license agreement or license certificate) on the basis of which the system is used.

About Kaspersky IoT Secure Gateway 1000 operating modes

In situations not covered by the standard operating scenarios of Kaspersky IoT Secure Gateway 1000, the system automatically switches to one of the following emergency modes: *non-immune mode*, *developer mode*, or *emergency support mode*.

Once activated, the mode name is displayed in the upper right corner on all pages of the Kaspersky IoT Secure Gateway 1000 web interface, and in the upper right corner of Kaspersky Security Center 14.2 Web Console after each synchronization. Click the mode name to view its description. Mode activation events are recorded in the [system audit log](#).

Non-immune mode

Non-immune mode is activated after you [start the VPN application](#) for the first time. When Kaspersky IoT Secure Gateway 1000 is operating in a non-immune mode, the device immunity is not guaranteed. However, there are no limitations to the functionality and operation of Kaspersky IoT Secure Gateway 1000.

The non-immune mode cannot be disabled in Kaspersky IoT Secure Gateway 1000 or the Kaspersky Security Center 14.2 Web Console. Exiting the non-immune mode is only possible after [a complete reinstallation of Kaspersky IoT Secure Gateway 1000](#) on the device.

Developer mode

Developer mode is activated after you start Kaspersky Debug Service (KDS) required for testing and debugging of components.

Kaspersky Debug Service is delivered with the Kaspersky IoT Secure Gateway 1000 SDK as a separate installation package. When Kaspersky Debug Service starts, developer mode is activated only for the user/developer who started the debug service.

If Kaspersky IoT Secure Gateway 1000 is operating in the developer mode, the application signatures are verified as follows when they are installed in Kaspersky IoT Secure Gateway 1000:

- If the application is installed using [Kaspersky IoT Secure Gateway 1000](#) or [Kaspersky Security Center 14.2 Web Console](#), the application signature is verified at all stages (download, installation, and launch of the application).
- If the application is installed via the KDS, the application signature is not verified.
- If the application is pre-installed in Kaspersky IoT Secure Gateway 1000, the application signature is not verified during the application launch. There are no download and installation stages since the application is pre-installed.

There are no limitations to the functionality of Kaspersky IoT Secure Gateway 1000.

The non-immune mode cannot be disabled through the Kaspersky IoT Secure Gateway 1000 web interface or Kaspersky Security Center 14.2 Web Console. Developer mode can only be exited after [completely reinstalling Kaspersky IoT Secure Gateway 1000](#) on the device where Kaspersky Debug Service was started.

Emergency support mode

Emergency support mode is activated when at least one of the following events occurs:

- Error as a result of [self-testing](#).
- Error during automatic [file integrity check](#) on startup.
- A security application, such as Kaspersky IoT Secure Gateway Network Protector, crashing.
Kaspersky IoT Secure Gateway Network Protector may crash if industrial protocol traffic filtering rules cannot be loaded or have not been defined, application self-diagnostics complete with an error, or the application is not responding.

The following happens when emergency support mode is activated:

- A message about the crash and its cause is recorded in the [system audit log](#). If emergency support mode was activated as a result of Kaspersky IoT Secure Gateway Network Protector crashing, a message about the crash is also recorded in the [firewall audit log](#).
- The user's active connection session is terminated.
- Stoppage of all running applications is initiated.
- If emergency support mode was activated as a result of Kaspersky IoT Secure Gateway Network Protector crashing, any traffic except service traffic that supports the functioning of Kaspersky IoT Secure Gateway 1000 and network connectivity as determined by [preset allow rules](#) is blocked.

The emergency support mode cannot be disabled in Kaspersky IoT Secure Gateway 1000 or Kaspersky Security Center 14.2 Web Console. You can exit the emergency support mode in the following ways:

- [Device reboot](#) (it is possible to re-enter emergency support mode).
- [Restoration from a backup copy](#).
- [Full reinstallation of Kaspersky IoT Secure Gateway 1000](#) on the device.

Configuring Kaspersky IoT Secure Gateway 1000

This section describes how to configure Kaspersky IoT Secure Gateway 1000.

This functionality is available to the [administrator](#) only.

Scenario: Quick Start for administrators

This section describes the sequence of steps that must be performed by the administrator to install and configure Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, and to establish a connection between them.

The scenario for installing Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center and configuring a connection between them consists of the following steps:

1 Installing Kaspersky Security Center

Download the Kaspersky Security Center 14.2 distribution package and install the full version of Kaspersky Security Center on the server. The distribution package of the full version of Kaspersky Security Center 14.2 includes the Kaspersky Security Center 14.2 Web Console. You are advised to select the standard installation. For detailed information on installing Kaspersky Security Center, please refer to the *Main installation scenario* section of the Kaspersky Security Center 14.2 Online Help Guide.

2 Configuring firewall rules

For the operating system firewall of the server where Kaspersky Security Center is installed, configure rules that allow Kaspersky IoT Secure Gateway 1000 to connect to the Kaspersky Security Center server over the TCP protocol via port 13294. For detailed information on configuring firewall rules, please refer to the relevant documentation on the operating system you are using.

3 Installing the Kaspersky IoT Secure Gateway 1000 administration web plug-in

In the Kaspersky Security Center 14.2 Web Console interface, [install the Kaspersky IoT Secure Gateway 1000 administration web plug-in](#). A ZIP archive containing the distribution package for the Kaspersky IoT Secure Gateway 1000 web plug-in is included in the [distribution kit](#).

4 Configuring connection of UEFI protection devices

On the Kaspersky Security Center Administration Server, enable use of port 13294 for the TCP protocol to configure the connection between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center. For detailed information on enabling port 13294 on the Kaspersky Security Center Administration Server, please refer to the *UEFI protection devices* section of the Kaspersky Security Center 14.2 Online Help Guide.

5 Turning on the Kraftway Rubezh-N device

[Turn on the Kraftway Rubezh-N device](#).

6 Connecting to the Kaspersky IoT Secure Gateway 1000 web interface

[Connect to the Kaspersky IoT Secure Gateway 1000 web interface](#) with the default name and password, and the administrator certificate.

7 Configuring Kaspersky IoT Secure Gateway 1000 settings

After connecting to the Kaspersky IoT Secure Gateway 1000 web interface, configure the following settings:

- [Connection to the external network and internal network](#)

- [Modem profile](#)

8 Creating and uploading a KSC server certificate

[Create a new KSC server certificate](#) and save it on the local device. In the Kaspersky IoT Secure Gateway 1000 web interface, [upload the KSC server certificate](#) for configuring a connection to the Kaspersky Security Center 14.2 Web Console.

9 Configuring a connection between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center

In the Kaspersky IoT Secure Gateway 1000 web interface, configure the [connection to Kaspersky Security Center](#).

10 Updating the Kaspersky IoT Secure Gateway 1000 root and user certificates

[Update](#) the root and user certificates.

11 Adding Kaspersky IoT Secure Gateway 1000 to the list of managed devices

Connect to the Kaspersky Security Center 14.2 Web Console and [add Kaspersky IoT Secure Gateway 1000 to the list of managed devices in Kaspersky Security Center](#).

12 Configuring traffic filtering in Kaspersky IoT Secure Gateway Network Protector

If you have Kaspersky IoT Secure Gateway Network Protector installed, [configure traffic filtering rules for industrial protocols](#) and [start the application](#). Until you configure and run Kaspersky IoT Secure Gateway Network Protector, transit traffic on the device will be blocked to ensure the security of connected devices.

You can also [configure traffic filtering rules](#) and [start the application](#) through Kaspersky Security Center 14.2 Web Console if you have connected Kaspersky IoT Secure Gateway 1000 to Kaspersky Security Center.

After these actions are completed, Kaspersky IoT Secure Gateway 1000 is ready to use. You can manage Kaspersky IoT Secure Gateway 1000 in the [web interface](#) or [Kaspersky Security Center 14.2 Web Console](#), and also [monitor audit events](#).

Scenario: Configuring access from an external network to internal network devices

This section describes the sequence of actions required to configure access from an external network to internal network devices using Kaspersky IoT Secure Gateway 1000.

Prior to configuration, make sure that the port to be used for connecting to the internal network device is open and accessible for connection on the device.

The access configuration scenario consists of the following steps:

1 Configuring routing of transit IP packets

On the external device from which you want to access devices on the internal network, configure routing of transit IP packets to the Kaspersky IoT Secure Gateway 1000 external network (WAN) port.

For details on configuring routing of transit IP packets on an external network device, please refer to the User Guide for the device.

2 Disabling masquerading

[Disable masquerading](#) for dynamic conversion of IP addresses of transit packets received by Kaspersky IoT Secure Gateway 1000 from a device on the external network.

3 Creating a rule for access from an external network

[Create a firewall allow rule](#) to allow packets from a device on the Kaspersky IoT Secure Gateway 1000 external network (WAN) to the device on the internal network.

The rule that has been created will be applied simultaneously to all available interfaces for connecting to the external network, including those for connecting to the external network via a built-in modem.

4 Creating rules for access from the internal network

[Create a firewall allow rule](#) to allow packets from the device on the Kaspersky IoT Secure Gateway 1000 internal network (LAN) to the device on the external network.

5 Check the connection to an internal network device.

On a device that resides in the external network, check the connection to a device on the internal network.

For more details on the options for checking the connection to other network devices, please refer to the User Guide for the device.

Access configuration is complete. You will be able to connect from the external network to devices residing within the internal network of Kaspersky IoT Secure Gateway 1000, for example, to export data from these devices or to configure their settings.

Managing accounts

This section contains information about configuring administrator and user accounts of Kaspersky IoT Secure Gateway 1000, as well as about configuring the settings for connecting to the Kaspersky IoT Secure Gateway 1000 web interface.

This functionality is available to the [administrator](#) only.

About account roles

Kaspersky IoT Secure Gateway 1000 has two account roles:

- **Administrator.** Has full access to all features, settings, and data in Kaspersky IoT Secure Gateway 1000.
- **User.** Has limited access to features.

By default, there is one administrator account in Kaspersky IoT Secure Gateway 1000. The administrator can [create](#) only one user account.

Creating additional accounts is not supported.

The table below describes the sections of the web interface that are available to the administrator and user.

Sections of the web interface available to the administrator and user

Web interface section	Administrator	User
Status	✓	✓

Events	✓	✓
Audit	✓	None
Users	✓	None
Applications	✓	Only view lists of installed and running applications and lists of application logs
Network	✓	None
Self-diagnostics	✓	None
Settings	✓	None
About product	✓	✓

Viewing information about accounts and connection settings

To view information about accounts and the settings for connecting to the Kaspersky IoT Secure Gateway 1000 web interface:

In the menu in the left part of the web interface page, select **Users** → **User settings**.

This opens a page displaying the following information:

- The **General settings** section displays the main connection settings configured in the system: the number of available attempts to connect to Kaspersky IoT Secure Gateway 1000 before a temporary lock, and the time (in minutes) during which you cannot connect to Kaspersky IoT Secure Gateway 1000 if you have entered incorrect credentials a (configurable) number of times.
- The **Root certificate** subsection displays information about the root certificate that is being used to securely connect to the web interface through a browser, and the validity period of that certificate.
- The **Administrator** section displays the administrator account credentials: name, credentials expiration date, and the certificate validity period.
- The **User** section displays the user account credentials: name, credentials expiration date, and the certificate validity period.

In this section, you can also configure the [settings for connecting to the web interface](#), update the [account credentials](#) and [connection certificates](#).

Configuring connection settings

You can configure the settings for connecting to the Kaspersky IoT Secure Gateway 1000 web interface for the administrator and the user: credentials validity period, system inactivity time before block, the number of possible authorization attempts, and others.

To configure connection settings:

1. In the menu in the left part of the web interface page, select **Users** → **User settings**.
2. In the **General settings** section, click **Edit**.

3. In the settings window that opens, specify the values of the necessary settings:

- **User credentials validity period** – the number of days during which the user and the administrator can use the user name and password to connect.

You can specify a value between 180 and 365 days. When the specified validity period expires, update the administrator and user credentials.

- **Idle period** – the time (in minutes) during which the connection session remains active when the administrator or user is inactive.

You can specify a value between 1 and 30 minutes. After the specified time, the connection session is terminated if the user or administrator is inactive.

- **Credential expiration message display period** – the number of days remaining until the administrator or user credentials expire when you start receiving notifications.

You can specify a value between 3 and 30 days. During the specified period, the user also receives a notification about their account credentials expiration.

- **Certificate expiration message display period** – the number of days remaining until the administrator certificate or user certificate expires when you start receiving notifications.

You can specify a value between 3 and 30 days. During the specified period, the user also receives a notification about their certificate expiration.

- **Number of failed login attempts** is the maximum number of the administrator's or the user's attempts to enter incorrect data when attempting to connect to the Kaspersky IoT Secure Gateway 1000 web interface.

You can specify a value between 3 and 10. After the specified number of unsuccessful authorization attempts, Kaspersky IoT Secure Gateway 1000 is temporarily blocked.

- **Lockout duration after unsuccessful login** is the time (in minutes) during which connection to the Kaspersky IoT Secure Gateway 1000 web interface is unavailable to the administrator or the user after several unsuccessful authentication attempts.

You can specify a value between 1 and 30 minutes. If you enter incorrect connection credentials several times, you can try to connect again after the specified time.

4. Click the **Save** button.

Connection settings for the Kaspersky IoT Secure Gateway 1000 web interface are updated

Creating a user account

You can create a Kaspersky IoT Secure Gateway 1000 user account by updating the default credentials and specifying the user certificate. The user can connect to the Kaspersky IoT Secure Gateway 1000 web interface and has limited access to the functionality. You can only create one user account.

To create a user account:

1. Connect the USB drive or USB token with the user certificate and certificate private key to the computer.
2. In the menu in the left part of the web interface screen, select **Users** → **User settings**.
3. In the **User** section, click the **Update credentials** button and perform the following actions in the data update window that opens:

a. If necessary, enter a new user name in the **User name** field.

The name can include English letters, numbers, and the special characters @. _ - only.

b. In the **Old password** field, enter the default user password. Default password for the user: **useruser**.

c. In the **New password** field, enter a new password.

The password must meet the following requirements:

- Eight or more unique characters
- No matches with previously used passwords.

d. In the **Confirm new password** field, enter the new password again.

e. Click the **Save** button.

The user account credentials are updated.

4. In the **User** section, click the **Update certificate** button.

5. In the user certificate update window that opens, click the **Select certificate** button and select the user certificate from the USB drive or USB token.

Only files in the CRT, CER, DER, or PEM format can be added as a certificate. The certificate hash is uploaded to Kaspersky IoT Secure Gateway 1000.

The user certificate must be signed with the root certificate uploaded into Kaspersky IoT Secure Gateway 1000. If the user certificate is signed with a different root certificate, first [update](#) the root certificate and administrator certificate as well.


6. Wait for a successful download and click **Save**.

A user account with the updated data is created. The user can use these credentials and the user certificate to [connect to the Kaspersky IoT Secure Gateway 1000 web interface](#).

Updating account credentials

You can update the administrator and user account credentials (name and password) for connecting to the Kaspersky IoT Secure Gateway 1000 web interface. Account credentials must be updated in the following cases:

- The current credentials are compromised.
- The credentials have expired.
- Credentials have to be updated regularly in accordance with the information security requirements of your organization.

If administrator or user account credentials are about to expire, a notification is displayed, the  icon appears in the menu on the left side of the screen next to the **Users** section, and a corresponding event is recorded in the [operating system audit log](#). The user also receives a notification about the account credentials expiration. If you do not update the account credentials, the following happens after their expiration:

- If the user account credentials have expired, the account is blocked and the user is not able to connect to the Kaspersky IoT Secure Gateway 1000 web interface until the administrator updates the credentials. The administrator receives a notification to update the user account credentials.
- If your administrator account credentials have expired, you are redirected to the account credentials update page when connecting to the Kaspersky IoT Secure Gateway 1000 web interface.

If an administrator or user account credentials expire during an active session, the session is terminated. Update the account credentials to get access.

Updating the administrator account credentials

To update the administrator name and password:

1. In the menu in the left part of the web interface screen, select **Users** → **User settings**.
2. In the **Administrator** section, click the **Update credentials** button.
3. In the update credentials window, do the following:
 - a. Enter a new administrator name if necessary.
The name can include English letters, numbers, and the special characters @. _ - only.
 - b. Enter your old administrator password, new password, and confirm the new password.
The new password must meet the following requirements:
 - Eight or more unique characters
 - No matches with previously used passwords.

To update the credentials expiration date, the password must be changed.

4. Click the **Save** button.
The administrator account credentials are updated.

Updating the user account credentials

To update the user name and password:

1. In the menu in the left part of the web interface screen, select **Users** → **User settings**.
2. In the **User** section, click the **Update credentials** button.
3. In the update credentials window, do the following:
 - a. Enter a new user name if necessary.
The name can include English letters, numbers, and the special characters @. _ - only.
 - b. Enter the old user password, new password, and confirm the new password.
The new password must meet the following requirements:

- Eight or more unique characters
- No matches with previously used passwords.

To update the credentials expiration date, the password must be changed.

4. Click the **Save** button.

The user account credentials are updated.

Managing connection certificates

The TLS encryption protocol ensures data transfer security using SSL connection certificates. An *SSL connection certificate* (hereinafter referred to as simply "certificate") is a block of data containing information about the certificate owner, the owner's public key, and the start and end dates of certificate validity.

The following certificates are required for securely connecting to the Kaspersky IoT Secure Gateway 1000 web interface through a browser.

- Administrator certificate when connecting to the Kaspersky IoT Secure Gateway 1000 web interface through an administrator account
- User certificate when connecting to the Kaspersky IoT Secure Gateway 1000 web interface through a user account
- The root certificate used for signing the administrator certificate and user certificate

Certificates can be issued by a special infrastructure on individual USB drives or tokens. In this case, to [renew the certificate](#), you need a USB drive or token with a set of valid certificates. You can also [create the required certificates manually](#) and use these to connect to the Kaspersky IoT Secure Gateway 1000 web interface.

Creating certificates manually

Creating a root certificate

A root certificate can be issued by a certification authority and is stored on a USB drive or token, or you can create one yourself by following the instructions below.

The root certificate [uploaded to Kaspersky IoT Secure Gateway 1000](#) will be used later to verify the administrator certificate and user certificate when connecting to the Kaspersky IoT Secure Gateway 1000 web interface.

A root certificate must be created on a trusted device in a secure environment ensuring that the device has no vulnerabilities and no Internet access.

Below is an example of using the OpenSSL utility to create a root certificate. For detailed information on using the utility, refer to the OpenSSL documentation.

To create a root certificate using the OpenSSL tool:

1. In the console, start the OpenSSL tool by running the following command:

```
openssl req -x509 -newkey rsa:4096 -keyout cert_key.pem -out cert.pem -days 365 -subj
"/C=RU/ST=Moscow/L=Moscow/O=SomeOrganization/OU=SomeUnit/emailAddress=test@example.com
-extensions v3_ca
```

where:

- -x509 – setting that indicates creation of a self-signed certificate. In this case, the standard public key infrastructure of the SSL and TLS protocols is used to manage keys and certificates.
- -newkey – setting that indicates the need to create a new certificate and a new key at the same time.
- rsa:4096 – setting that defines the type and length of the key. When this setting is applied, a key will be created using the RSA encryption algorithm with a length of 4096 bits.
- -keyout cert_key.pem – name of the file where the private key of the created certificate is saved.
- -out cert.pem – name of the file where the created certificate is saved.
- -days 365 – this setting defines the validity term of the created root certificate.
- -subj – in this group of settings the registration information about the company that issued the certificate must be specified.

2. Enter and confirm the password for the private certificate key. The password must differ from the default [certificate](#) password.

As a result, the following two files are created in the directory where the command was executed:

- cert.pem: root certificate file
- cert_key.pem: root certificate private key

The newly created cert.pem root certificate file must be uploaded, if the [root certificate needs to be updated](#).

Creating an administrator certificate and user certificate

An administrator certificate and user certificate can be created from a previously generated root certificate.

The administrator certificate and user certificate [uploaded to Kaspersky IoT Secure Gateway 1000](#) will then be used to connect to the Kaspersky IoT Secure Gateway 1000 web interface.

Below is an example of using the OpenSSL utility to create an administrator certificate or user certificate. For detailed information on using the utility, refer to the OpenSSL documentation.

To create an administrator certificate or user certificate using the OpenSSL tool:

1. To create a new certificate, run the OpenSSL utility in the console by executing the following command:

```
openssl req -new -newkey rsa:4096 -keyout TlsClientAdminKey.pem -out
TlsClientAdmin.csr
```

2. To sign the certificate with the previously generated root certificate, run the following command and enter the password for the root certificate private key:

```
openssl x509 -req -days 365 -in TlsClientAdmin.csr -CA cert.pem -CAkey cert_key.pem -
CAcreateserial -out TlsClientAdmin.crt -extensions v3_req
```

The new certificate file in CRT format is needed for [updating the administrator certificate or user certificate](#).

3. To create an archive containing the new certificate and private key, run the following command:

```
openssl pkcs12 -export -in TlsClientAdmin.crt -inkey TlsClientAdminKey.pem -out TlsClientAdmin.p12 -name TlsClientAdmin -descert -nomaciter
```


The new archive file in P12 format must be uploaded to the browser when [connecting to the Kaspersky IoT Secure Gateway 1000 web interface](#).

Updating certificates

To connect securely to the Kaspersky IoT Secure Gateway 1000 web interface through a browser, you need an administrator certificate, a user certificate, and the root certificate that was used to sign the administrator certificate and user certificate.

You have to update certificates in the following cases:

- Current certificates have been compromised.
- Certificates have expired.
- Certificates need to be regularly updated in accordance with the information security requirements of your organization.

If an administrator certificate or user certificate is about to expire, the appropriate notification is displayed, the  icon appears in the menu on the left side of the screen next to the **Users** section, and the corresponding event is recorded in the [operating system audit log](#). The user also receives a notification about the certificate expiration. After the certificate expires, the following happens:

- If the user certificate has expired, the account is blocked and the user is not able to connect to the Kaspersky IoT Secure Gateway 1000 web interface. The active connection session is terminated. You receive a prompt to update the user certificate.
- If the administrator certificate has expired, the account is blocked and the administrator is not able to connect to the Kaspersky IoT Secure Gateway 1000 web interface.
- If the root certificate has expired, you need to update all certificates: the root certificate, administrator certificate, and user certificate.

When updating the certificate, you may have to restart the browser to clear the cache of the current Kaspersky IoT Secure Gateway 1000 connection session.

Loading widely known Certification Authority certificates is not recommended, as all servers that use certificates signed by these Certification Authority certificates will be trusted. This situation can lead to Kaspersky IoT Secure Gateway 1000 being compromised.

Using USB tokens

You can use USB tokens with a certificate key 4096 bits or 8192 bits of length to connect to the Kaspersky IoT Secure Gateway 1000 web interface.

To use a USB token:

1. Connect a USB token to the computer that is used for connecting to the Kaspersky IoT Secure Gateway 1000 web interface.
2. Install the software supplied for supporting the USB token operation.
3. Export the token certificate using this software.
4. Upload the exported certificate to Kaspersky IoT Secure Gateway 1000 as an administrator or user certificate, as described below.

Updating a root certificate

Before updating the root certificate, upload to the browser the .p12 archive containing the administrator certificate signed with the new root certificate. You can find the instructions on how to upload the certificate in the browser documentation.

Updating the root certificate is not possible in Mozilla Firefox browser starting from version 124. For more details on supported browsers, refer to the ["Hardware and software requirements"](#) section.

To update the root certificate information, do as follows:

1. If the new root certificate is stored on a USB drive or token, connect it to the computer on which you are connected to the Kaspersky IoT Secure Gateway 1000 web interface.
2. In the menu in the left part of the web interface page, select **Users** → **User settings**.
3. In the **Root certificate** subsection, click **Update certificate**.
4. In the certificate update window, click **Select certificate**, and in the window that opens, select a valid root certificate file.
Only files in the CRT, CER, DER, or PEM format can be added as a certificate. The certificate hash is uploaded to Kaspersky IoT Secure Gateway 1000.
5. Wait for a successful download and click **Save**.

Information about the uploaded root certificate and its validity period is displayed in the **Root certificate** subsection. After that, update the administrator certificate and user certificate that are signed with the new root certificate.

After updating the root certificate, the administrator certificate must be renewed before disconnecting from the Kaspersky IoT Secure Gateway 1000 web interface.

Updating an administrator certificate

To update the administrator certificate:

1. If the new administrator certificate is stored on a USB drive or token, connect it to the computer on which you are connected to the Kaspersky IoT Secure Gateway 1000 web interface.

2. In the menu in the left part of the web interface page, select **Users** → **User settings**.
3. If the new administrator certificate is signed with a different root certificate, follow the preceding instructions to upload the required root certificate.

In this case, update also the user certificate, so that the user can connect to the Kaspersky IoT Secure Gateway 1000 web interface.
4. In the **Administrator** section, click the **Update certificate** button.
5. In the certificate update window, click **Select certificate**, and in the window that opens, select a valid administrator certificate file.

Only files in the CRT, CER, DER, or PEM format can be added as a certificate. The certificate hash is uploaded to Kaspersky IoT Secure Gateway 1000.
6. Wait for a successful download and click **Save**.

The information about the administrator certificate is updated, and the information about the previously uploaded certificate is deleted. The connection session is terminated, [reconnect to the Kaspersky IoT Secure Gateway 1000 web interface](#).

After updating the administrator certificate, if you also have updated the root certificate, remove the administrator certificate signed with the old root certificate from the browser. You can find the instructions on how to remove the certificate in the browser documentation.

Updating a user certificate

To update the user certificate:

1. If the new user certificate is stored on a USB drive or token, connect it to the computer on which you are connected to the Kaspersky IoT Secure Gateway 1000 web interface.
2. In the menu in the left part of the web interface page, select **Users** → **User settings**.
3. If the new user certificate is signed with a different root certificate, follow the preceding instructions to upload the required root certificate.
4. In the **User** section, click the **Update certificate** button.
5. In the certificate update window, click **Select certificate**, and in the window that opens, select a valid user certificate file.

Only files in the CRT, CER, DER, or PEM format can be added as a certificate. The certificate hash is uploaded to Kaspersky IoT Secure Gateway 1000.
6. Wait for a successful download and click **Save**.

The information about the user certificate is updated, and the information about the previously uploaded certificate is deleted. The user can use the updated certificate to [connect to the Kaspersky IoT Secure Gateway 1000 web interface](#).

Configuring the web server

Operation of the Kaspersky IoT Secure Gateway 1000 web interface is supported by a CivetWeb web server. Web server settings are stored in a configuration file, connection security is ensured by the web server certificate. Kaspersky IoT Secure Gateway 1000 is delivered with a predefined web server certificate signed by Kaspersky.

You have to update the web server certificates in the following cases:

- Current certificates have been compromised.
- [The IP address of Kaspersky IoT Secure Gateway 1000](#) has changed.


After the first connection, replace the web server certificate installed by default with the certificate used in your organization.

To upload a new web server certificate:

1. In the menu in the left part of the web interface page, select **Users** → **Web server settings**.

A page opens showing the information about the certificate and web server key.

2. Do one of the following:

- If you have not added a certificate, click **Upload certificate**.
- If you have already added a certificate and want to replace it, click the pencil icon  in the upper right corner of the certificate information section.

3. In the **Upload web server certificate** window that opens, do the following:

a. In the **Certificate** field, click the **Select certificate** button, and in the download window that opens, select the certificate file in the CRT, CER, DER, or PEM format.

Make sure that when the web server certificate is generated, the Kaspersky IoT Secure Gateway 1000 IP address in the local network is specified as the value of the subjAltName parameter.

b. In the **Certificate key** field, click the **Select a certificate key** button, and in the download window that opens, select the key file in the KEY format.

c. Click **Save** to save the changes.

4. Refresh the page for the new certificate to take effect.

If you have already uploaded the certificate and key, they are replaced.

In the **Users** → **Web server settings** section, the following information about the certificate used is displayed:

- Certificate file name and its format.
- **Subject name** – information about the application for which the certificate is issued.
- **Issuer** – information about the organization that issued the certificate.
- **Certificate validity period** – certificate expiration date.

Configuring network settings

Kaspersky IoT Secure Gateway 1000 is delivered with the statically configured IP address 192.168.1.1, which you can [change](#) if required. To enable the system to operate as an Internet of Things (IoT) Secure Gateway, configure the settings of the internal and external network.

You can also configure the following network settings for transferring the data:

- Network address translation, or *masquerading* (enable or disable);
- Modem profile for cellular connection on the device running Kaspersky IoT Secure Gateway 1000 (if the modem is connected to the device);
- Routing for more flexible management of network packets that pass through the device with Kaspersky IoT Secure Gateway 1000;
- An MQTT broker for telemetry data exchange over the MQTT (Message Queuing Telemetry Transport) protocol.

You can view and change the Kaspersky IoT Secure Gateway 1000 network settings in the **Network** section on the corresponding tabs.

This functionality is available to the [administrator](#) only.

Configuring the LAN settings

An *internal network* (LAN) is an enterprise network in which sensors transmit telemetry data to the system. The Kaspersky IoT Secure Gateway 1000 internal network can be used to carry out the following tasks:

- [Connect to the Kaspersky IoT Secure Gateway 1000 web interface.](#)
- [Forward event logs to an internal Syslog server.](#)
- Communicate with internal network devices connected to Kaspersky IoT Secure Gateway 1000, such as sensors.

If the Kaspersky IoT Secure Gateway 1000 IP address on the internal network changes, the web interface connection session is closed. [Reconnect to Kaspersky IoT Secure Gateway 1000](#) at the new IP address.

When the network mask of Kaspersky IoT Secure Gateway 1000 in the internal network is changed, you must reconfigure the internal network settings.

When the **Use DHCP server** feature is enabled or disabled, you must restart Kaspersky IoT Secure Gateway 1000.

To configure the LAN settings:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. On the **LAN** tab, specify values for the following settings:
 - **IP address.** The default value of this parameter is 192.168.1.1.
 - **Subnet mask.** The default value of this parameter is 255.255.255.0.

The **MAC address** field displays the MAC address of the system in the internal network.

3. If you want to configure network settings automatically via DHCP for the devices in the internal network, set the **Use DHCP server** toggle button to Enabled and specify values for the following settings:
 - **Start of IP address range.**
 - **End of IP address range.**
 - **Primary DNS server address.** The default value of this parameter is 8.8.8.8.
 - **Secondary DNS server address.** The default value of this parameter is 8.8.4.4.

By default, the **Use DHCP server** toggle button is switched on.

4. If you want to configure network settings manually for the devices in the internal network, set the **Use DHCP server** toggle button to Disabled.
5. Click **Save** in the lower part of the page to save the changes.
6. [Restart](#) Kaspersky IoT Secure Gateway 1000 to apply the changes to the network settings.

Configuring masquerading

You can configure the network address translation using the masquerading function.

Masquerading is a type of network address translation, in which the sender's address in the internal network is dynamically replaced with an address in the external network, depending on the address assigned to the interface. You can use the masquerading functionality if you need to spoof the parameters in the headers of IP packets for devices on the internal network or to hide an infrastructure behind one address. This will allow devices that reside in the internal network and do not have real IP addresses to send and receive IP packets from an external network.

To enable masquerading:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. On the **WAN** tab, in the **Broadcast settings** subsection, toggle on **Enable masquerading**.
Masquerading will be applied only to the communication channel designated as main ([external network](#) or [modem](#)).

Configuring the WAN settings

An *external network* is a network used by Kaspersky IoT Secure Gateway 1000 to access the Internet or to interact with Kaspersky Security Center. The Kaspersky IoT Secure Gateway 1000 external network can be used to carry out the following tasks:

- [Configure interaction between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center.](#)
- [Forward event logs to an external Syslog server.](#)

To configure the WAN settings:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. On the **WAN** tab in the **External network settings** section, do one of the following:
 - If you need to configure network settings automatically using the DHCP protocol, set the **Automatic (via DHCP)** toggle button to the enabled position. The **Automatic (via DHCP)** toggle button is switched on by default.

If the DHCP server issues null DNS server addresses to Kaspersky IoT Secure Gateway 1000 when enabling automatic configuration of external network settings, connection to resources and routing by domain name will be unavailable. In that event, turn off automatic configuration of network settings over the DHCP and manually set the primary and secondary DNS server addresses.

- If you need to manually configure the network settings, set the **Automatic (via DHCP)** toggle button to the disabled position and specify the values for the following settings:
 - **IP address.** By default, this is set to the last address received from the DHCP server. If there is no such address, this is set to the [IP address of the internal network](#) (192.168.1.1 by default).
 - **Subnet mask.** The default value of this parameter is 255.255.255.0.
 - **Gateway.**
 - **Primary DNS server address.**
 - **Secondary DNS server address.**

The **MAC address** field displays the MAC address of the system in the external network.

3. Click **Save** to save the changes.
4. [Restart](#) Kaspersky IoT Secure Gateway 1000 to apply the changes to the network settings.

Configuring cellular connection settings

If the device does not have a modem, the cellular connection is unavailable and its settings are hidden.

Cellular connectivity for devices running Kaspersky IoT Secure Gateway 1000 is provided by a HUAWEI ME909s-120 or SIMCom SIM7600 modem. The cellular connection settings are saved in the modem profile. Kaspersky IoT Secure Gateway 1000 is delivered with predefined modem profiles that include a configuration file containing basic scripts for configuring a cellular connection. A modem profile configuration file must also contain modem AT commands that establish and maintain a connection, and a description of the settings for configuring PPP (Point-to-Point Protocol).

You can view and configure the cellular connection settings under **Network** → **WAN**. The section contains the **Modem settings** section, which provides the following information about the cellular connection:

- Modem operation status and the current signal level.
- The **Modem DNS server addresses** section shows the IP addresses of the primary and secondary DNS servers of the modem.
- The **Profiles** table displays information about the available modem profiles.



Kaspersky IoT Secure Gateway 1000 allows you to [create new modem profiles](#), [edit the existing profiles](#), and [switch between profiles](#). Different modem profiles enable you to work with different cellular communication providers. To use a cellular connection, one of the modem profiles must be active. One of the predefined modem profiles is active by default.

Modem profiles table


The system provides two types of modem profiles:

- *Predefined profile* – a profile provided together with the device. Predefined profiles are read-only.
- *Custom profile* – a profile that is created during configuration of the cellular connection. Custom profiles can be edited and deleted.

Information about the modem profiles is displayed in the **Network** → **WAN** → **Modem settings** section, in the **Profiles** table. The table shows the following information for each modem profile:

-  – profile editing access. This icon indicates that a profile is read-only and is only displayed for predefined profiles.
- Active – the  icon indicates that the modem profile is currently being used.
- **Name** – name of the profile.
- **Modified** – date and time of the most recent profile update.

You can view and edit the settings of the selected profile by clicking the plus  icon on the left of the profile name. The following information is displayed for each file in the **Profile settings** table:

-  – configuration file editing access. This icon, indicating that the configuration file is read-only, is only displayed for the configuration file of the predefined profile.
- **Type** – type of configuration file.
- **Name** – name of the configuration file.
- **Modified** – date and time of the most recent change in the configuration profile.

Enabling and disabling a cellular connection

Kaspersky IoT Secure Gateway 1000 lets you process outgoing and incoming network traffic using a cellular connection (through a cellular communications provider).

To enable or disable the use of a cellular connection on a device running Kaspersky IoT Secure Gateway 1000:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab. In the **Modem settings** subsection, enable or disable the modem by means of the **Use modem as main communication channel** toggle switch.
3. Click **Save** to save the changes made to the settings.

Creating a modem profile

You can create new modem profiles. Different modem profiles enable you to work with different cellular communication providers.

To create a new modem profile:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab.
3. In the **Modem settings** section, click the **Create** button at the bottom of the page.
The **Create modem profile** pane opens on the right.
4. In the **Template** drop-down list, select the modem profile that you want to use as the basis for creating the new profile. The modem configuration file of the selected profile is added to the new profile.
If you want to create an empty profile, select **None** in the **Template** drop-down list. You can [complete the empty modem profile](#) at a later time.
5. In the **Name** field, enter the profile name using letters of the English alphabet.
6. Click **Save** in the lower part of the page to save the changes.

The new modem profile will be created and will appear in the **Profiles** table.

Copying a modem profile

You can copy a previously created or predefined modem profile if you need to create a new modem profile based on an existing profile and do not need to make changes to the settings of the new profile.

To copy a previously created modem profile:

1. In the menu in the left part of the web interface page, select the **Network** section.

2. Select the **WAN** tab.

3. In the lower part of the window, in the **Profiles** table, in the **Name** column, click the name of the profile that you want to use to create the new profile.

The **Edit modem profile** pane opens on the right.

4. Click the  icon in the lower part of the pane.

The **Copy modem profile** pane opens.

5. In the **New name** field, enter the new profile name using letters of the English alphabet.

6. Click **Copy** in the lower part of the pane.

The new modem profile based on the previously created profile will be created and will appear in the **Profiles** table.


Completing an empty modem profile

A profile is empty if it was [created](#) from the **None** template and has no configuration file. An empty profile must be completed before it can be used.

To complete an empty modem profile:

1. In the menu in the left part of the web interface page, select the **Network** section.

2. Select the **WAN** tab.

3. In the **Modem settings** subsection, in the **Profiles** table, click the plus icon  in the **Name** column next to the name of the empty profile.

The **Profile settings** table will be displayed.

4. Click **Create file** to create a modem configuration file.

5. In the **Create modem configuration file** pane that opens on the right, in the **Name** field, enter the name of the configuration file using letters of the English alphabet.

6. Click **Save** to save the modem configuration file.

The **Create modem configuration file** pane closes.

7. If you need to upload a prepared modem configuration file, click the **Upload** button in the lower part of the page. In the opened file upload window, select a configuration file.

The configuration file will be uploaded to the system and will appear in the profile settings.

We do not recommend downloading or creating more than one configuration file per modem profile. When uploading or creating a new file, the previously uploaded configuration file will be overwritten.

8. If you need to change the settings of the configuration file, in the profile settings table click the name of the configuration file that was just created or uploaded.

The **Edit modem configuration file** pane opens on the right.

9. In the lower part of the pane, click the pencil  icon.

This opens a text editor window for editing the configuration file.

10. Type the required modem configuration file settings in the text editor window.
11. Click **Save** in the lower part of the page to save the changes.

Editing a modem profile



You can change the name and settings of a modem profile.

To change the name of a modem profile:


1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab.
3. In the **Modem settings** section, in the **Profiles** table, in the **Name** column, click the name of the profile that you want to edit.
The **Edit modem profile** pane opens on the right.
4. In the **Name** field, enter a new profile name.
5. Click **Save** to save the changes made to the settings.

The modified modem profile will be displayed in the **Profiles** table.

To change the modem profile settings:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab.
3. In the **Modem settings** subsection, in the **Profiles** table, click the plus icon  in the **Name** column next to the profile that you want to edit.
This opens the **Profile settings** table containing a list of configuration files and certificates that are part of the profile. If the profile was created based on the **None** template, the list of files will be empty. An empty profile must be [completed](#).
4. If you need to edit a configuration file, click the name of the configuration file and do the following in the **Edit modem configuration file** pane that opens on the right:
 - a. Click the  icon in the lower part of the pane.
 - b. In the opened text editor window, change the modem settings as required.
 - c. Click **Save** in the lower part of the page to save the changes.

The selected configuration file will be changed. The text editor window closes.

5. If you need to delete a configuration file, click the name of the configuration file and click the  icon located in the lower part of the **Edit modem configuration file** pane that opens on the right. Confirm file deletion.
The selected configuration file will be deleted from the modem profile settings.

6. If you need to upload a prepared modem configuration file, click the **Upload** button in the lower part of the page. In the opened file upload window, select a configuration file.

The configuration file will be uploaded to the system and will appear in the profile settings.

We do not recommend downloading or creating more than one configuration file per modem profile. When uploading or creating a new file, the previously uploaded configuration file will be overwritten.

Switching to a different modem profile

Kaspersky IoT Secure Gateway 1000 lets you switch between modem profiles. Different modem profiles enable you to work with different cellular communication providers. One of the predefined modem profiles is active by default.


To switch to a different modem profile:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab.
3. In the **Modem settings** section, in the **Profiles** table, in the **Name** column, click the name of the profile that you want to set as active.

The **Edit modem profile** pane opens on the right.

4. In the lower part of the pane, click the **Set as active** button.

5. [Restart](#) Kaspersky IoT Secure Gateway 1000 to apply the changes.

In the **Profiles** table, in the **Active** column, the  icon appears next to the selected profile. The profile is now active and will be used when connecting to the network.

Deleting a modem profile


You can delete a modem profile.

Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined modem profiles. If you need to delete the profile that is currently the active profile, you must first [switch to a different modem profile](#).

To delete a modem profile:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **WAN** tab.
3. In the **Modem settings** section, in the **Profiles** table, in the **Name** column, click the name of the profile that you want to delete.

The **Edit modem profile** pane opens on the right.

4. Click the  icon in the lower part of the pane and confirm profile deletion.

The selected modem profile will be deleted from the **Profiles** table.

Configuring routing

You can configure routing for more flexible management of network packets that pass through a device with Kaspersky IoT Secure Gateway 1000. *Routing* is the process of defining the path traveled by data in communication networks.

Data transfer using static routes for the internal network is possible only for the [network router device type](#).

The **Network** section on the **Routing** tab shows the routing table of Kaspersky IoT Secure Gateway 1000. The following information is displayed for each route in the table:

- **Type** – type of route:
 - **Static** – route for which the settings for routing network packets were manually defined.
 - **Dynamic** – route for which the settings for routing network packets are automatically determined by using a DHCP server, for example.
- **IP address** – IP address of the destination node or network.
- **Mask** – destination network mask.
- **Gateway** – IP address of the gateway in the network to which you need to transmit the traffic on the way to the specified IP address of the destination node or network.
- **Status** – route state:
 - **Active** – the route was applied and is used for data transmission.
 - **Error** – the route was not applied and cannot be used for data transmission because an error was made when creating the route. The error description is displayed on the right of the state.
The **Error** state is displayed if the IP address of the gateway in the network is unreachable or if an invalid IP address or network mask was indicated as the destination node or network.
 - **Pending** – intermediate state that is assigned if the route was created via the Kaspersky Security Center 14.2 Web Console. After the route settings are validated, the current state is changed to **Active** or **Error**.
- **Edit** and **Delete** – actions that you can perform for the selected route. Only static routes are available for editing and deletion.

You can also [create](#), [edit](#) and [delete](#) routes of Kaspersky IoT Secure Gateway 1000.

The routing table is updated automatically every 30 seconds. The new routes that were [created via the Kaspersky Security Center 14.2 Web Console](#) are displayed in the table after it is updated. If necessary, you can force an update of the routing table by clicking the **Reload table** button.

Creating a static route

You can create new static routes that will let you forward network traffic as required by the infrastructure of your organization.

Kaspersky IoT Secure Gateway 1000 does not let you create duplicate default routes (second route for the IP address of the destination network 0.0.0.0/0) and routes in which an IP address in the network 127.0.0.0/8 is indicated as the IP address of the destination node.

When creating overlapping routes, you are advised to keep in mind that the route with the longer mask describing a smaller number of destination nodes will be selected to send a network packet to the IP address of the destination node or network.

To create a new static route:

1. In the menu in the left part of the web interface page, select the **Network** section.

2. Select the **Routing** tab.

The lower part of the opened window contains the routing table of Kaspersky IoT Secure Gateway 1000.

3. Click the **Add route** button.

4. In the opened **Add route** window, enter the following data:

- In the **IP address** field, enter the IP address of the destination node or network.
- In the **Mask** field, enter the destination network mask.
- In the **Gateway** field, enter the IP address of the gateway. The gateway IP address must be reachable.
The gateway IP address is reachable if this IP address resides within a connected network and is one of the nodes of a network configured on the internal or external interface.

5. Click **Save** in the lower part of the window to save the changes.

The new static route is created and displayed in the routing table.

Editing a static route

To edit a static route:

1. In the menu in the left part of the web interface page, select the **Network** section.

2. Select the **Routing** tab.

This opens a window containing the routing table of Kaspersky IoT Secure Gateway 1000.


3. In the **Edit** column, click the  icon for the route that you want to edit.

4. In the opened **Edit route** window, make the necessary changes and click **Save** to save your changes.

The static route is changed, and the new data on this route is displayed in the routing table.

Deleting a static route

To delete a static route:

1. In the menu in the left part of the web interface page, select the **Network** section.
2. Select the **Routing** tab.
This opens a window containing the routing table of Kaspersky IoT Secure Gateway 1000.
3. In the **Delete** column, click the  icon and confirm deletion for the route that you want to delete.

The static route will be deleted from the routing table.

Configuring MQTT broker settings

Configuration of the MQTT broker settings is available only to the [network router device type](#).

In Kaspersky IoT Secure Gateway 1000, the Eclipse Mosquitto MQTT broker exchanges telemetry data over the Message Queuing Telemetry Transport (MQTT) protocol. MQTT settings are stored in an MQTT broker profile. An MQTT broker profile binds an Eclipse Mosquitto configuration file to security certificates. Kaspersky IoT Secure Gateway 1000 is delivered with a predefined profile that includes an MQTT broker configuration file. Kaspersky IoT Secure Gateway 1000 lets you [create new profiles](#), [edit existing profiles](#), and [switch between profiles](#). To transmit data over the MQTT protocol, one of the MQTT broker profiles must be active. The predefined profile is active by default.

The MQTT broker does not support a TLS connection for traffic coming from controllers and sensors of internal enterprise network hardware. A TLS connection is supported only for external network traffic.



When configuring MQTT broker settings, the contents of the configuration file may contain personal data. You need to check the data uploaded to the MQTT broker profile of Kaspersky IoT Secure Gateway 1000.

Table of MQTT broker profiles


Kaspersky IoT Secure Gateway 1000 provides for two types of MQTT broker profiles:


- *Predefined profile* – a profile provided together with the device. Predefined profiles are read-only and cannot be edited or deleted.
- *Custom profile* – profile that was created during configuration of the MQTT broker. Custom profiles can be edited and deleted.

The information about MQTT broker profiles is provided as a table in the **Network** → **MQTT broker** section. The table shows the following information for each MQTT broker profile:

-  – profile editing access. This icon indicates that a profile is read-only and is only displayed for predefined profiles.
- **Active:** the  icon indicates that the MQTT broker profile is currently in use.
- **Name** – name of the profile.

- **Modified** – date and time of the most recent change in the profile.

You can view the settings of a selected profile by clicking the  icon on the left of the profile name. The following information is displayed for each file in the **Profile settings** table:

-  – configuration file editing access. This icon, indicating that the configuration file is read-only, is only displayed for the configuration file of the predefined profile.
- **Type** – type of configuration file.
- **Name** – name of the configuration file.
- **Modified** – date and time of the most recent change in the configuration profile.

Creating an MQTT broker profile

You can create new MQTT broker profiles. Different MQTT broker profiles let you work with different servers and digital platforms that receive events from Kaspersky IoT Secure Gateway 1000 over the MQTT protocol.

To create a new MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. Click the **Create new** button in the lower part of the page.

The **Create MQTT broker profile** pane opens on the right.

3. In the **Template** drop-down list, select the MQTT broker profile that you want to use as the basis for creating the new profile.

The Eclipse Mosquitto configuration file and security certificates of the selected profile are added to the new profile.

If you want to create an empty profile, select **None** in the **Template** drop-down list. You can [complete](#) the empty profile at a later time.

4. In the **Name** field, enter the profile name using letters of the English alphabet.

5. Click **Save** in the lower part of the page to save the changes.

The new MQTT broker profile is created and appears in the profile table. You can also [create an MQTT broker profile](#) from the Kaspersky Security Center 14.2 Web Console.

Copying an MQTT broker profile

You can copy a previously created or predefined MQTT broker profile if you need to create a new MQTT broker profile based on an existing profile and do not need to make changes to the settings of the new profile.


To copy a previously created MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the name of the profile that you want to edit.

The **Edit MQTT broker profile** pane opens on the right.

3. Click the  icon in the lower part of the pane.

The **Copy MQTT broker profile** pane opens.

4. In the **New name** field, enter the new profile name using letters of the English alphabet.

5. Click **Copy** in the lower part of the pane.

The new MQTT broker profile based on the previously created profile is created and appears in the profile table. The Eclipse Mosquitto configuration file and security certificates of the selected profile are added to the new profile.

Completing an empty MQTT broker profile

An MQTT broker profile is empty if it was created from the **None** template and has not yet been completed. The settings of an empty profile do not show any configuration files or certificates.

To complete an empty MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the  icon next to the profile that you want to complete.

The **Profile settings** table will be displayed.

3. Add a security certificate to the MQTT broker profile by clicking **Upload** in the lower part of the page. In the file upload window that opens, select a certificate file in CER, CRT, PEM, or DER format. The file size must not exceed 131 KB.

The certificate file will be uploaded to the system and will appear in the MQTT broker profile settings.

An MQTT broker profile requires multiple security certificates, such as a certificate issued by a Certificate Authority, a server client certificate, and a private key file. Depending on the requirements of the MQTT server, the server client certificate and private key file must be signed with a valid certificate issued by a certification authority. If your profile prescribes the use of SSL/TLS, repeat this step as many times as required to upload all required certificates to the system. A secure connection is not guaranteed in the absence of security certificates.

We do not recommend uploading more than three security certificate files per MQTT profile. If more than three files are uploaded, only the last uploaded certificate files will be used.

4. Create a configuration file in the MQTT broker profile by clicking the **Create new file** button.

The **Create MQTT broker configuration file** pane opens on the right.

5. In the **Name** field, enter the name of the configuration file using letters of the English alphabet.

6. Click **Save** to save the Eclipse Mosquitto MQTT broker configuration file.

The **Create MQTT broker configuration file** pane closes. A configuration file will be created. You can create only one configuration file.

You can create only one configuration file. If it needs to be replaced, you need to [delete the active configuration file](#) and then re-create it. You can only set an MQTT profile as active if it has a configuration file added.

7. In the **Profile settings** table, click the name of the configuration file that was just created.

8. In the lower part of the **Edit MQTT broker configuration file** pane that opens on the right, click the  icon.

This opens a text editor window for editing the configuration file.

9. In the text editor window, enter the required settings of the Eclipse Mosquitto MQTT broker configuration file.

For detailed information on the settings of the Eclipse Mosquitto MQTT broker configuration file, please refer to the documentation on the [developer's website](#). There are [limitations](#) when configuring the MQTT broker for Kaspersky IoT Secure Gateway 1000.

10. If you need to add a prepared configuration file to the profile, click the **Upload** button in the lower part of the page. In the opened file upload window, select a file in CONF format.

The configuration file will be uploaded to the system and will appear in the MQTT broker profile settings.

11. Click **Save** in the lower part of the page to save the changes.

Modifying an MQTT broker profile

You can change the name and settings of an MQTT broker profile.

Kaspersky IoT Secure Gateway 1000 does not let you change the predefined MQTT broker profile.

For a profile currently set as active, you can edit the name only. If you need to change active profile settings, you have to [switch to a different MQTT broker profile](#) first.

To change the name of an MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the name of the profile that you want to edit.

The **Edit MQTT broker profile** pane opens on the right.

3. In the **Name** field, enter a new profile name.

4. Click **Save** in the lower part of the page to save the changes.

The modified MQTT broker profile will appear in the **Profiles** table.

To change the settings of the MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the  icon next to the profile that you want to edit.

This opens the **Profile settings** table containing a list of configuration files and certificates that are part of the MQTT broker profile. If the profile was created based on the **None** template, the list of files will be empty. An empty profile must be [completed](#).

If the profile is active or predefined, you cannot edit its settings. For an active profile, you can edit the name only.

3. If you need to add a prepared configuration file to the profile, click the **Upload** button in the lower part of the page. In the opened file upload window, select a file in CONF format.

The configuration file will be uploaded to the system and will appear in the MQTT broker profile settings.

4. If you need to change the name of the configuration file, click the name of the configuration file and in the **Edit MQTT broker configuration file** pane that opens on the right, provide a new name in the **Name** field and click **Save**.

5. If you need to edit a configuration file in the MQTT broker profile, click the name of the configuration file that you want to edit and do the following in the **Edit MQTT broker configuration file** pane that opens on the right:

- a. Click the  icon in the lower part of the pane.

- b. In the opened text editor window, change the settings as required.

For detailed information on the settings of the Eclipse Mosquitto configuration file, please refer to the documentation on the [developer's website](#)²⁴. There are [limitations](#) when configuring the MQTT broker profile for Kaspersky IoT Secure Gateway 1000.

- c. Click **Save** in the lower part of the page to save the changes.

The selected configuration file will be changed. The text editor window closes.

6. If you need to delete a configuration file from the MQTT broker profile, click the name of the configuration file and click the  icon located in the lower part of the **Edit MQTT broker configuration file** pane that opens on the right. Confirm file deletion.


The selected configuration file will be deleted from the MQTT broker profile settings.

7. If you need to add a security certificate to the MQTT broker profile, click **Upload** in the lower part of the page. In the file upload window that opens, select a certificate file in CER, CRT, PEM, or DER format. The file size must not exceed 131 KB.

The certificate file will be uploaded to the system and will appear in the MQTT broker profile settings.

An MQTT broker profile requires multiple security certificates, such as a certificate issued by a Certificate Authority, a server client certificate, and a private key file. Depending on the requirements of the MQTT server, the server client certificate and private key file must be signed with a valid certificate issued by a certification authority. If your profile prescribes the use of SSL/TLS, repeat this step as many times as required to upload all required certificates to the system. A secure connection is not guaranteed in the absence of security certificates.

We do not recommend uploading more than three security certificate files per MQTT profile. If more than three files are uploaded, only the last uploaded certificate files will be used.

8. If you need to remove a security certificate from the profile, click the name of this certificate in the **Profile settings** table and click the  icon in the pane that opens on the right. Confirm certificate removal.

The selected security certificate file will be deleted from the MQTT broker profile settings.

Switching to a different MQTT broker profile

Kaspersky IoT Secure Gateway 1000 lets you switch between MQTT broker profiles. In Kaspersky IoT Secure Gateway 1000, different MQTT broker profiles let you work with different servers and digital platforms when receiving telemetry data from them over the MQTT protocol. The predefined MQTT broker profile is active by default.

You can set an MQTT broker profile as active only if it contains a configuration file.

To switch to a different MQTT broker profile:


1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the name of the profile that you want to set as active.

The **Edit MQTT broker profile** window opens.

3. In the lower part of the opened window, click the **Set as active** button.

In the profile table, in the **Active** column, the  icon appears next to the selected profile. The profile is now active and is used by Kaspersky IoT Secure Gateway 1000 when receiving data over the MQTT protocol.

Deleting an MQTT broker profile

Kaspersky IoT Secure Gateway 1000 lets you delete MQTT broker profiles.

Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined MQTT broker profile. If you need to delete the profile that is currently the active profile, you must first [switch to a different MQTT broker profile](#).


To delete an MQTT broker profile:

1. In the menu in the left part of the web interface page, select the **Network** section and then the **MQTT broker** tab.

This opens a table that lists the MQTT broker profiles.

2. In the **Name** column, click the name of the profile that you want to delete.

The **Edit MQTT broker profile** pane opens on the right.

3. Click the  icon in the lower part of the pane and confirm profile deletion.

The selected MQTT broker profile is deleted from the profile table.

Limitations when configuring an MQTT broker

[Connections to local devices](#) are made without using a TLS protocol. Connections to devices on an external network are made using a TLS protocol.

Kaspersky IoT Secure Gateway 1000 supports configuration of the MQTT broker Eclipse Mosquitto settings with the following limitations:

- It is not permitted to use the `capath`, `bridge_capath` and `include_dir` options for assigning the path to file locations.
- It is not permitted to use the TLS protocol to configure a connection of equipment with Kaspersky IoT Secure Gateway 1000.

The following parameters are not supported when configuring a connection with Kaspersky IoT Secure Gateway 1000 from the internal network: `cafile`, `certfile`, `ciphers_tls1.3`, `crlfile`, `dhparamfile`, `keyfile`, `require_certificate`, `tls_engine`, `tls_engine_kpass_sha1`, `tls_keyform`, `use_identity_as_username`, `use_subject_as_username`, `psk_hint`.

- It is required to use the TLS protocol for connection of Kaspersky IoT Secure Gateway 1000 with devices or cloud services in the external network.

The following options are not supported when configuring a connection: `bridge_insecure` (always false), `bridge_alpn`, `bridge_capath`, `bridge_cafile`, `bridge_certfile`, `bridge_keyfile`, `bridge_identity`, `bridge_psk`, `bridge_require_ocsp`, `bridge_tls_version`.

- There can be a connection with only one client application for each MQTT broker profile (you can indicate only one `bridge` parameter in the configuration file). Simultaneous operations with multiple client connections are not supported. To establish a connection with another client, you must [switch to a different MQTT broker profile](#).
- The following options are not supported when configuring an MQTT broker profile: `bridge_require_ocsp`, `log_dest_file`, `pid_file` and `http_dir`, `persistence`, `websockets`, `auth_plugin`, `password_file`.
- When configuring an MQTT broker profile, you must use the `allow_anonymous` option.
- To connect the MQTT broker to a digital platform that supports the MQTT protocol, you must specify the standard port 8883 for the connection.
- Port 1883 must be used to connect an end user device to Kaspersky IoT Secure Gateway 1000.

Filtering application protocol traffic

You can set up application protocol traffic filtering in the web interface of Kaspersky IoT Secure Gateway 1000. Filtering allows blocking or unblocking FTP, HTTP, MQTT, Modbus, SMTP, IMAP, and POP3 traffic.

For the MQTT protocol only version 3.1.1 filtering is supported. For SMTP protocol only basic SMTP filtering is supported. Extended SMTP protocol filtering is not supported.

To configure application protocol traffic filtering:

1. In the menu on the left side of the screen, select the **Network** → **Filtering** section.
2. Configure traffic filtering for application protocols as follows:
 - Select the check box next to the protocols for which you want to block traffic.
 - Clear the check box next to the protocols for which you want to allow traffic.

By default, traffic is allowed for all application protocols.

3. Click the **Save** button.

Kaspersky IoT Secure Gateway 1000 blocks all traffic for selected application protocols except for service traffic and allows traffic for the application protocols for which you cleared the check box.

When receiving a traffic packet that contains signs of a blocked application protocol, Kaspersky IoT Secure Gateway 1000 terminates the connection through which this traffic was exchanged. Several packets required to establish a connection may pass through Kaspersky IoT Secure Gateway 1000 after the traffic is detected, but then the connection will be terminated.

Adding device name

To add a device name:

1. In the menu in the left part of the web interface page, select **Settings** → **General**.
2. Enter the name in the **Device name** field.

The device name can contain only numbers and letters of the English alphabet. The maximum name length is 32 characters.
3. Click **Save** to save the changes.

Configuring the date and time

You can configure the date and time in Kaspersky IoT Secure Gateway 1000.

To configure the date and time:

1. In the menu in the left part of the web interface page, select **Settings** → **General**.
2. In the **Date and time** subsection, specify the current date and time:

- Click the date and in the drop-down calendar, select the current day, month, and year.
You can go to the selection of the month and the year by clicking the date at the top of the calendar.
 - Click the time and on the drop-down clock, select the current time in hours and minutes.
Indicate the current time in the UTC+00:00 time zone. The time is displayed according to the time zone of the device.
3. Click **Save** to save the changes.

Configuring delivery of notifications when registering events

This section contains information about configuring notifications to be sent when [events](#) are registered in Kaspersky IoT Secure Gateway 1000.

Configuring delivery of event logs to the Syslog server

Kaspersky IoT Secure Gateway 1000 can forward [firewall and system audit logs](#) to a Syslog server.

To configure forwarding of firewall and system audit logs to a Syslog server:

1. In the menu in the left part of the web interface page, select **Settings** → **Notifications**.
2. In the **Syslog** group of settings, toggle **Use Syslog server to send events** on.
3. Configure how event logs are forwarded by specifying the following settings:
 - In the **IP address and port** field, enter the IP address and port of the recipient Syslog server like in the following example: `198.51.100.0:514`.
 - In the **Mode** drop-down list, select the protocol to be used by Kaspersky IoT Secure Gateway 1000 to forward event logs to the external Syslog server:
 - **UDP**.
 - **TCP**.
 - **TCP/TLS**.
 - If the **TCP/TLS** protocol is selected for forwarding logs, upload a security certificate. To do so, click the **Upload new certificate** button and select the relevant security certificate in the opened window.
4. Click **Save** to save the changes.

Configuring delivery of MQTT notifications

Kaspersky IoT Secure Gateway 1000 can send notifications about [firewall and system audit events](#) over the MQTT protocol.

To configure delivery of MQTT notifications:

1. In the menu in the left part of the web interface page, select **Settings** → **Notifications**.
2. In the **MQTT notifications** group of settings, enable sending MQTT notifications by enabling the **Use MQTT to send events** option.
3. Configure the settings for forwarding MQTT notifications:
 - a. In the **IP address** field, enter the IP address of the MQTT broker you are using.
 - b. In the **Port** field, enter the port number of the MQTT broker you are using.

You can use ports 1883 and 8883 to connect Kaspersky IoT Secure Gateway 1000 to an MQTT broker residing in an internal network.

You can use port 8883 to connect Kaspersky IoT Secure Gateway 1000 to an MQTT broker residing in an external network.

- c. In the **MQTT topic name** field, specify the name of the MQTT-topic for sending notifications about events.
 - d. If you need to send notifications about events from a specific user, set the **Use authentication** toggle button to the enabled position and provide the following data:
 - In the **User name** field, enter the user login name for authorization on the server.
 - In the **Password** field, enter the password of the user login for authorization on the server.

You can obtain the user account credentials from the system administrator. Sending notifications from a specific user is disabled by default.
 - e. If you need to use a secure SSL connection, set the **Use secure SSL connection** toggle button to the enabled position and do the following:
 1. Upload a certificate issued by a Certificate Authority. To do so, click the **Upload certificate** button and select a certificate file on the local device.

Information about the uploaded certificate from a Certificate Authority will be displayed on the page.

Loading widely known Certification Authority certificates is not recommended, as all servers that use certificates signed by these Certification Authority certificates will be trusted. This situation can lead to Kaspersky IoT Secure Gateway 1000 being compromised.
 2. Upload the client certificate. To do so, click the **Upload client certificate** button and select a certificate file on the local device.

Information about the uploaded client certificate will be displayed on the page.
 3. Upload a key for the client certificate. To do so, click the **Upload key** button and select a key file on the local device.

Use of a secure SSL connection is disabled by default.
4. Click **Save** in the lower part of the page to save the changes.

Configuring Kaspersky Security Center Administration Server settings

This section contains information about managing certificates and configuring the settings for connecting to the Kaspersky Security Center Administration Server.


Creating a Kaspersky Security Center Administration Server certificate

The TLS encryption protocol ensures data transfer security using SSL connection certificates. An *SSL connection certificate* (hereinafter referred to as simply "certificate") is a block of data containing information about the certificate owner, the owner's public key, and the start and end dates of certificate validity.

A KSC server certificate is required for securely connecting to Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console. For detailed information about the requirements applied to KSC server certificates, please refer to the section titled *Requirements for user certificates in Kaspersky Security Center* in the Kaspersky Security Center 14.2 Online Help Guide.

You can issue a new KSC server certificate in the Kaspersky Security Center 14.2 Web Console.

To issue a new KSC server certificate through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Kaspersky Security Center 14.2 Web Console, click the  icon next to the name of the relevant Kaspersky Security Center Administration Server.

The **Administration Server properties** window opens.

2. Select the **Certificates** section.

3. In the **Administration Server authentication by UEFI protection devices** settings block, select **Certificate issued through Administration Server**.

4. Click the **Reissue** button.

5. In the opened window, configure the connection address:

- [Use old connection address](#) 

The address of the Administration Server to which Kaspersky IoT Secure Gateway 1000 connects will remain the same.

This option is selected by default.

- [Change connection address to](#) 


If you need Kaspersky IoT Secure Gateway 1000 to connect to a different address, specify the relevant address in this field.

6. Click **OK** to save the changes.

The new KSC server certificate will be issued.

To upload a Kaspersky Security Center certificate file to Kaspersky IoT Secure Gateway 1000, the Kaspersky Security Center certificate file that was created through the web interface of the Kaspersky Security Center 14.2 Web Console must be saved on the local computer.

To save a Kaspersky Security Center certificate file that was created in the Kaspersky Security Center 14.2 Web Console:

1. In the web interface menu of the Kaspersky Security Center 14.2 Web Console, click the  icon next to the name of the relevant Kaspersky Security Center Administration Server.
The **Administration Server properties** window opens.
2. Select the **Certificates** section.
3. In the **Administration Server authentication by UEFI protection devices** settings group, select **Certificate issued through Administration Server**.
4. Click the **Manage certificate** button.
5. In the opened pane on the right, in the **Connection address** block, click the IP address of Kaspersky IoT Secure Gateway 1000 for which the certificate was issued.

The certificate file will begin to automatically download.

In Kaspersky IoT Secure Gateway 1000, you can download a Kaspersky Security Center certificate file only in CRT, CER, DER or PEM format. If necessary, you can use the OpenSSL tool to change the format of a Kaspersky Security Center certificate file. For example, to change the format of a certificate file from P12 to CRT, run the following command in the console:

```
openssl pkcs12 -in <certificate name>.p12 -clcerts -nokeys -out <certificate name>.crt
```

A created KSC server certificate file needs to be [added](#) to Kaspersky IoT Secure Gateway 1000 to [configure a connection with Kaspersky Security Center](#).

Updating a Kaspersky Security Center Administration Server certificate

You must update the KSC server certificate in the following cases:

- The current certificate is compromised.
- The certificate has expired.
- The IP address of the device running Kaspersky IoT Secure Gateway 1000 has changed.
- Certificate need to be regularly updated in accordance with the information security requirements of your organization.

Loading widely known Certification Authority certificates is not recommended, as all servers that use certificates signed by these Certification Authority certificates will be trusted. This situation will lead to Kaspersky IoT Secure Gateway 1000 being compromised.

To add or remove a certificate:

1. In the menu in the left part of the web interface page, select **Settings** → **Administration Server**.

On the **Kaspersky Security Center Administration Server** page that opens, the **Certificate** section displays data about the current Kaspersky Security Center Administration Server certificate (if loaded).

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

- If you need to upload a KSC server certificate, click **Upload** and select the certificate file in the opened window.
Only files in the CRT, CER, DER, or PEM format can be added as a certificate.
The new KSC server certificate will be uploaded to the system and the previously uploaded certificate will be deleted.
- If you need to delete the KSC server certificate, click the **Delete** button and confirm deletion.

If there is no KSC server certificate in the system, it is not possible to [configure the settings for connecting to the Kaspersky Security Center server](#) or to connect to the Kaspersky Security Center server.

Configuring the settings for connecting to Kaspersky Security Center

To securely manage Kaspersky IoT Secure Gateway 1000 from the Kaspersky Security Center 14.2 Web Console, configure the Kaspersky Security Center Administration Server connection settings.

If there is no [KSC server certificate](#) in the system, it is not possible to configure the settings for connecting to the Kaspersky Security Center Administration Server.

To configure the settings for connecting to Kaspersky Security Center Administration Server:

1. In the menu in the left part of the web interface page, select **Settings** → **Administration Server**.
The **Kaspersky Security Center Administration Server** connection settings page opens.
2. In the **Connection settings** section, in the **Domain address** field, enter the domain address of the Kaspersky Security Center Administration Server you are connecting to.
The **Port** field indicates the port number used for the connection. You cannot edit the connection port number.
3. Click **Save** in the lower part of the page to save the changes.

Modifying the configuration of Kaspersky IoT Secure Gateway 1000 manually.

You can view and directly reconfigure Kaspersky IoT Secure Gateway 1000. Configuration settings in plain text are **key: value** pairs in JSON format. The list of the main configuration keys is shown in the table below.

To view and edit the Kaspersky IoT Secure Gateway 1000 configuration, do as follows:

1. In the Kaspersky IoT Secure Gateway 1000 web interface, go to **Settings** → **Configuration**.
The tab that opens displays the current configuration of Kaspersky IoT Secure Gateway 1000 in JSON format.

2. If required, edit the parameters in the configuration field.

The fields and parameters in the configuration field are case sensitive. Respect the specified case when adding or editing fields or parameters.

3. Click **Save** to apply the new configuration settings.

Manual reconfiguration may cause malfunctions in Kaspersky IoT Secure Gateway 1000 up to the point where a full reinstallation is required. It is recommended to change the configuration settings by using the corresponding settings in the Kaspersky IoT Secure Gateway 1000 web interface and the Kaspersky Security Center Web Console.

Main configuration keys

Key name	Value type	Title	Required	Possible values
ABOUT	Object	Object containing information about the Kaspersky IoT Secure Gateway 1000 version and the SDK version.	Yes	-
text	String	Information about versions.	No	String indicating the version of Kaspersky IoT Secure Gateway 1000 and SDK, for example: "text": "Kaspersky IoT Secure Gateway**\n\nVersion: 3.0.0.0\n\nKaspersky SDK version: 3.0.0.332"
<Application package name>	Object	Application configuration details. Required only for applications that contain a configuration	No	Package name from the package_id field of an application-related set Example: kaspersky.kisg.net for Kaspersky IoT Secure Network Protector .
<Any name>	Any type	Application configuration content	No	Application configuration content
APPLICATIONS	Object	Information about installed applications.	Yes	APPLICATIONS object
MARKETPLACE	Object	Object containing	Yes	Populated automatically from the application manifest

			the list of applications available to install .		
	apps_requested	List of strings	List of applications available from the application marketplace	No	
	package_id	String	Application package identifier	Yes, if apps_requested contains at least one record	
	requested_state	String	Action requested from the application		
	buildSdkVersion	String	Platform version		
	kosappversion	String	Application version.		
MODE_SWITCH		Object	Object that contains information about the current state of the Kaspersky IoT Secure Gateway 1000 operating modes and the network device type	No	-
	is_developer_mode	Literal	Developer mode.	No	true: developer mode on false: developer mode off
	is_no_secure_mode	Literal	Insecure mode	No	true: insecure mode on false: insecure mode off
	router_mode	Literal	Network device type You can change the network device type only by reinstalling Kaspersky IoT Secure Gateway 1000.	No	true: device type – network router false: device type – unidirectional gateway
MQTT		Object	Object containing	Yes	MQTT/LIST/profileList
	LIST	Object			

				MQTT broker settings		
		<code>profileList</code>	Object list	Object list containing MQTT broker profile settings		
<code>NETWORK</code>			Object	Object containing network settings	Yes	NETWORK object
<code>SETTINGS</code>			Object	Object containing general Kaspersky IoT Secure Gateway 1000 settings.	Yes	SETTINGS object

APPLICATIONS object

Manual reconfiguration may cause malfunctions in Kaspersky IoT Secure Gateway 1000 up to the point where a full reinstallation is required. We recommend changing the configuration by means of the relevant settings in the Kaspersky IoT Secure Gateway 1000 web interface and the Kaspersky IoT Secure Gateway 1000 management web plug-in for Kaspersky Security Center 14.2 Web Console.

`APPLICATIONS` includes keys containing [information about installed applications](#) and their settings in Kaspersky IoT Secure Gateway 1000. The list of these keys is shown in the table below.

List of APPLICATIONS keys

Key name	Value type	Title	Required	Possible values
<code>APPS_CONTROL</code>	Object	Object containing list of installed applications and their settings.	Yes	-
<code>applications</code>	Object list	A list of objects containing application settings.	Yes	-
<code>configured</code>	Literal	A flag that indicates whether the application is	No	<code>true</code> means the application is configured; <code>false</code> means the application

				configured or not.		is not configured.
		<code>execute</code>	Literal	The flag that enables the application to be started.	Yes, if <code>applications</code> contains at least one record	<code>true</code> means the application will be started; <code>false</code> means the application will not be started.
		<code>restart_on_failure</code>	Literal	The flag that enables the application to be restarted after an abrupt termination.		<code>true</code> means auto-restart mode is active; <code>false</code> means auto-restart mode is inactive.
		<code>state</code>	Integer	Application status.	No	<code>0</code> means the application is starting <code>1</code> means application is running <code>4</code> means the application is stopped <code>5</code> means the application is stopping
		<code>subtype</code>	String	Application subtype.		Retrieved automatically from application data.
		<code>ksc_plugin_ui_content</code>	String	Content to display in the Kaspersky Security Center 14.2 Web Console management web plug-in.		
		<code>ksc_plugin_md5</code>	String	A content checksum to display in the Kaspersky Security Center 14.2 Web Console		

				management web plug-in.		
		<code>manifest</code>	String	The content of the application manifest.		
		<code>package_id</code>	String	The application package name.	Yes, if <code>applications</code> contains at least one record	
		<code>launchRule</code>	String	Application start rule.		<code>forbidden</code> means the application is forbidden from starting; <code>auto</code> means the application has an autorun feature; <code>none</code> means that no special startup rules apply to the application.
		<code>logLevel</code>	Integer	The current logging level of application messages.	Yes	<code>0</code> : critical messages, <code>1</code> : error messages, <code>2</code> : warning messages, <code>3</code> : informational messages, <code>4</code> : debug messages, <code>5</code> : all application actions. Each subsequent logging level includes messages from the previous level.
		<code>version</code>	String	Application version.	No	Retrieved automatically from application data.
		<code>name</code>	String	Application name.		
		<code>type</code>	String	Application type.		
		<code>APPS_ROUTING</code>	Object	An object containing a list of available application routes.	Yes	-
		<code>routes</code>	Object list	List of routes	Yes	-

		<code>active</code>	Literal	A flag that indicates route active status.	Yes, if <code>routes</code> contains at least one record	<code>true</code> means the route is active; <code>false</code> means the route is inactive.
		<code>destination</code>	Object	Route destination object		-
		<code>application_id</code>	String	Application identifier		Retrieved automatically from application data.
		<code>endpoint</code>	String	Application endpoint name.		
		<code>source</code>	Object	Route source object		-
		<code>application_id</code>	String	Application identifier		Retrieved automatically from application data.
		<code>endpoint</code>	String	Application endpoint name.		

Application settings that contain configuration are configured in separate objects that correspond to the `package_id` value. For example, [the settings for filtering industrial protocol traffic](#) in Kaspersky IoT Secure Gateway Network Protector are located in `kaspersky.kisg.netprotector`.

MQTT/LIST/profileList object list

Manual reconfiguration may cause malfunctions in Kaspersky IoT Secure Gateway 1000 up to the point where a full reinstallation is required. We recommended changing the configuration by means of the relevant settings in the Kaspersky IoT Secure Gateway 1000 web interface and the Kaspersky IoT Secure Gateway 1000 management web plug-in for Kaspersky Security Center 14.2 Web Console.

The `MQTT/LIST/profileList` object list includes keys containing the [MQTT broker profile settings](#). The list of these keys is shown in the table below.

List of keys for describing the MQTT broker profile instance in the `MQTT/LIST/profileList` object list

Key name	Value type	Title	Required	Possible values
<code>fileList</code>	Object list	List of profile files	Yes, if <code>profileList</code> contains at least one record	-
<code>fileContent</code>	String	Base64-encoded	Yes, if <code>fileList</code>	Obtained automatically from the file

			content of the profile file.	contains at least one record	
	<code>name</code>	String	Profile file name		Obtained automatically from the file path
	<code>type</code>	String	Profile file type		<code>main_conf_file</code> : main configuration file; <code>cert_file</code> : file containing the certificate; <code>key_file</code> : file containing the key
	<code>uuid</code>	String	Unique ID of the profile file	No	String representation of <code>boost::uuids::uuid</code> .
<code>locked</code>		String	The profile is blocked.	No	Determined automatically from the <code>predefined</code> and <code>status</code> fields
<code>modified</code>		String	Date and time of the most recent change in the profile.	Yes	Obtained automatically from the file
<code>name</code>		String	Profile name.	Yes	Arbitrary string value
<code>predefined</code>		Literal	Predefined	Yes	<code>true</code> : predefined profile; <code>false</code> : custom profile
<code>status</code>		String	Profile status	Yes	<code>active</code> : profile active; <code>inactive</code> : profile inactive
<code>uuid</code>		String	Profile unique ID	No	String representation of <code>boost::uuids::uuid</code> .

NETWORK object

Manual reconfiguration may cause malfunctions in Kaspersky IoT Secure Gateway 1000 up to the point where a full reinstallation is required. We recommended changing the configuration by means of the relevant settings in the Kaspersky IoT Secure Gateway 1000 web interface and the Kaspersky IoT Secure Gateway 1000 management web plug-in for Kaspersky Security Center 14.2 Web Console.

The `NETWORK` object includes keys containing [network settings](#). The list of these keys is shown in the table below.

List of NETWORK keys

Key name	Value type	Title	Required	Possible value
<code>APP_PROTO</code>	Object	Network protocol filtering settings .	Yes	-
<code>filtered_protos</code>	Object	Object containing information about network protocol filtering	Yes	-
<code>ftp</code>	Literal	FTP protocol	Yes	<code>true</code> : protocol filterir

				filtering		enabled; <code>false</code> : protocol filtering disabled.
		<code>http</code>	Literal	HTTP/HTTPS protocol filtering	Yes	
		<code>imap</code>	Literal	IMAP protocol filtering	Yes	
		<code>modbus</code>	Literal	Modbus protocol filtering	Yes	
		<code>mqtt</code>	Literal	MQTT protocol filtering Only MQTT protocol version 3.1.1 filtering is supported.	Yes	
		<code>pop3</code>	Literal	POP3 protocol filtering	Yes	
		<code>smtp</code>	Literal	SMTP protocol filtering Only basic SMTP protocol filtering is supported.	Yes	
<code>CARP</code>			Object	Network cluster settings .	Yes	-
		<code>advskew</code>	Integer	Priority of Kaspersky IoT Secure Gateway 1000 in the cluster	Yes	From <code>0</code> to <code>254</code> , where maximum priority and the minimum priority.
		<code>clusterId</code>	String	Cluster identifier. This is required for cluster nodes to uniquely recognize each other. The use of the ID does not guarantee protection against the actions of third parties. When setting up the network, you also need to secure the cluster network loop.	Yes	Cluster identifier. To avoid ID overlap, we recommend specifying a custom <code>clusterId</code> value.
		<code>enabled</code>	Literal	Enables or	Yes	<code>true</code> : network cluster

				disables the network cluster.		enabled; <code>false</code> : network cluster disabled.
	<code>ip</code>	String	Cluster IP address.	Yes		String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ip": "192.168.110.120"</code>
	<code>mask</code>	String	Cluster subnet mask.	Yes		String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"mask": "255.255.255.0"</code>
FIREWALL		Object	Firewall rules.	Yes		-
	<code>rules</code>	Object list	List of firewall rules. The maximum size of the list is 512 objects.	Yes		-
	<code>status</code>	Literal	Enables or disables firewall rules.	Yes, if <code>rules</code> contains at least one record		<code>true</code> : the rule is on; <code>false</code> : the rule is off.
	<code>action</code>	String	Rule type			<code>accept</code> : allow rule; <code>deny</code> : deny rule.
	<code>ipAddrSource</code>	String	Source IP address.			String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ipAddrSource": "192.168.110.125"</code>
	<code>ipAddrDest</code>	String	Destination IP address.			String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ipAddrDest": "192.168.110.126"</code>
	<code>portSource</code>	String	Source port			Number that defines the source port
	<code>portDest</code>	String	Target port			Number that defines the target port
	<code>protocol</code>	String	Communication protocol			Available rule options: <code>any, icmp, tcp, udp</code>
	<code>zone</code>	String	Rule scope			Available rule options: <code>In, Out</code>
IDS_PROXY		Object	Settings for address denylists and allowlists Used only if Kaspersky IoT Secure Gateway Network Protector is installed.	Yes		-

	<code>IPSPFlag</code>	Literal	Enables or disables address denylists and allowlists.	Yes	<code>true</code> : lists enabled; <code>false</code> : lists disabled
	<code>IPSPStatusFlag</code>	Literal	Flag that indicates the active status of address denylists and allowlists.	No	Always set to <code>true</code>
	<code>blockedList</code>	Object list	List of denied addresses.	Yes	-
	<code>ipAddrSource</code>	String	Denied IP address.	Yes, if <code>blockedList</code> contains at least one record	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ipAddrSource192.168.1.201"</code>
	<code>timestamp</code>	Date and time	Timestamp		POSIX timestamp
	<code>signatureName</code>	String	Name of the signature that was blocked		Signature name
	<code>blockedListFlag</code>	Literal	Enables or disables access to resources on the list of blocked addresses	Yes	<code>true</code> : access to resources disabled; <code>false</code> : access to resources enabled
	<code>allowList</code>	Object list	Address allowlist.	Yes	-
	<code>ipAddrSource</code>	String	Allowed IP address.	Yes, if <code>allowList</code> contains at least one record	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ipAddrSource192.168.1.200"</code>
<code>LAN</code>		Object	Internal network settings .		Yes
	<code>DHCPFlag</code>	Literal	Enables or disables automatically obtaining an IP address over DHCP.	Yes	<code>true</code> : automatic obtaining of an IP address enabled; <code>false</code> : automatic obtaining of an IP address disabled
	<code>FirstDHCPAddress</code>	String	DHCP server primary IP address	Yes	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"FirstDHCPAddress192.168.1.20"</code>
	<code>FirstDNSServer</code>	String	DNS server primary IP address	Yes	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"FirstDNSServer192.168.1.20"</code>

					"FirstDNSServer": "192.168.1.20"
	IP	String	Internal network adapter IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "IP": "192.168.1.1"
	LastDHCPAddress	String	DHCP server secondary IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "LastDHCPAddress" "192.168.1.40"
	MAC	String	Internal network adapter MAC address	No	String formatted as XX:XX:XX:XX:XX:XX example: "MAC": "1A:2B:3C:4D:5E:6"
	Mask	String	Internal network subnet mask	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "Mask": "255.255.255.0"
	SecondDNSServer	String	DNS server secondary IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "SecondDNSServer" "192.168.1.40"
NAPT		Object	Masquerading rules	Yes	-
	rules	Object list	List of masquerading rules The maximum size of the list is 256 rules.	Yes	-
	comment	String	Comments to the rule	Yes, if rules contains at least one record	Arbitrary string
	ipAddrInternal	String	Internal network host IP address		String formatted as XXX.XXX.XXX.XXX, f example: "ipAddrInternal": "192.168.1.4"
	portExternal	Integer	External port		Number that defines t external port
	portInternal	Integer	Internal port		Number that defines t internal port
	protocol	String	Rule protocol		Available rule options: udp
	zone	String	Interface to which the rule is applied.		Available rule options: wan
NAT		Object	Turns masquerading	Yes	-

	<code>masquerading</code>	Literal	on or off.	Yes	<code>true</code> : masquerading enabled <code>false</code> : masquerading disabled
<code>ROUTING_TABLE</code>		Object	Routing table	Yes	-
	<code>routes</code>	Object list	List of routes	Yes	-
	<code>action</code>	String	Route action	Yes, if <code>routes</code> contains at least one record	<code>add</code> : add route; <code>delete</code> : delete route; <code>no action</code> : no action required
	<code>ipaddr</code>	String	IP address.	Yes, if <code>routes</code> contains at least one record and the <code>action</code> key value is not equal to <code>no action</code>	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"ipaddr": "192.168.2.1"</code>
	<code>mask</code>	String	Subnet mask.		String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"mask": "255.255.255.0"</code>
	<code>gateway</code>	String	Gateway IP address.		String formatted as <code>XXX.XXX.XXX.XXX</code> , for example: <code>"gateway": "192.168.1.100"</code>
	<code>state</code>	String	Route status.	No	<code>failed</code> : an error occurred while performing an action on the route; <code>active</code> : the route is active; <code>pending</code> : no action is being performed on the route
	<code>type</code>	String	Route type.	No	<code>static</code> : static route; <code>dynamic</code> : dynamic route
	<code>error</code>	String	Error message	No	Message about an error that occurred while performing an action on the route
<code>WAN</code>		Object	External network settings .	Yes	-
	<code>DHCPFlag</code>	Literal	Enables or disables automatically obtaining an IP address over DHCP.	Yes	<code>true</code> : automatic obtaining of an IP address enabled <code>false</code> : automatic obtaining of an IP address disabled
	<code>DefaultGateway</code>	String	IP address of the default gateway.	Yes	String formatted as <code>XXX.XXX.XXX.XXX</code> , for example:

					"DefaultGateway": "192.168.1.111"
	FirstDNSAddress	String	DNS server primary IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "FirstDNSServer": "8.8.8.8"
	IP	String	External network adapter IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "IP": "192.168.1.1"
	MAC	String	External network adapter MAC address	No	String formatted as XX:XX:XX:XX:XX:XX example: "MAC": "1A:2B:3C:4D:5E:6"
	Mask	String	External subnet mask	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "Mask": "255.255.255.0"
	SecondDNSAddress	String	DNS server secondary IP address	Yes	String formatted as XXX.XXX.XXX.XXX, f example: "SecondDNSServer": "8.8.4.4"

SETTINGS object

Manual reconfiguration may cause malfunctions in Kaspersky IoT Secure Gateway 1000 up to the point where a full reinstallation is required. We recommended changing the configuration by means of the relevant settings in the Kaspersky IoT Secure Gateway 1000 web interface and the Kaspersky IoT Secure Gateway 1000 management web plug-in for Kaspersky Security Center 14.2 Web Console.

The **SETTINGS** object includes keys containing the Kaspersky IoT Secure Gateway 1000 general settings. The list of these keys is shown in the table below.

List of SETTINGS keys

Key name	Value type	Title	Required	Possible values
AUTH_CERTS	Object	Information about user , application , web server and Kaspersky Security Center certificates.	Yes	-
certificate_admin	String	Administrator certificate.		Certificate in format
certificate_admin_name	String	Administrator		Name of the f

			certificate name		containing the certificate
	certificate_app_ca	String	Application root certificate		Certificate in format
	certificate_app_ca_name	String	Application root certificate name		Name of the file containing the certificate
	certificate_app_cl	String	Application client certificate		Certificate in format
	certificate_app_cl_key	String	Application client certificate key		Key in Base64
	certificate_app_cl_key_name	String	Application client certificate key name		Name of the file containing the
	certificate_app_cl_name	String	Application client certificate name		Name of the file containing the certificate
	certificate_ksc_server	String	Kaspersky Security Center certificate.		Certificate in format
	certificate_ksc_server_name	String	Kaspersky Security Center certificate name.		Name of the file containing the certificate
	certificate_web_tls	String	Web server certificate.		Certificate in format
	certificate_web_tls_key	String	Web server certificate key.		Key in Base64
	certificate_web_tls_key_name	String	Web server certificate key name.		Name of the file containing the
	certificate_web_tls_name	String	Web server certificate name.		Name of the file containing the certificate
DEVICE		Object	Device name.	Yes	-
	device_name	String			Device name in Kaspersky Security Center
KSC		Object	Object containing information about communications with Kaspersky Security Center	Yes	-
	command	String	A command prepared to send to	No	reboot : reboot device

			Kaspersky IoT Secure Gateway 1000.		
	heartbeat	Integer	Period of synchronization with Kaspersky Security Center, in seconds		Integer
MODEM		Object	Information about the modem and settings for telecom carriers.	Yes	-
	connection_quality	Integer	Indicator of the current connection quality	No	Received auto
	connection_status	String	Communication status	No	on means the is connected; transmitting d means the mc present in the but the conne inactive; na m modem is not in the system; means the sta unknown.
	is_enable	Literal	Turns the modem on or off.	Yes	true: modem false: mode
	primary_dns	String	Primary DNS server	No	String format: XXX.XXX.XXX example: "primary_dr "8.8.8.8"
	profileList	Object list	List of mobile network operator profiles	Yes	-
	fileContent	String	Profile file content	Yes	Obtained auto from the profi
	locked	String	Indicates whether the profile is read-only	No	Determined fr predefined status fields
	modified	String	Date and time of the most recent change in the profile.	Yes	Date and time
	name	String	Profile name.		Arbitrary nam

						profile.
		<code>predefined</code>	Literal	Flag that indicates whether the profile is predefined		<code>true</code> : predefined profile; <code>false</code> : profile
		<code>status</code>	String	Current status of the profile		<code>active</code> : profile active; <code>inactive</code> : profile inactive
		<code>uuid</code>	String	Profile unique ID	No	String representation of <code>boost::uuid</code>
	<code>secondary_dns</code>		String	Secondary DNS server	No	String format: <code>XXX.XXX.XXX</code> example: <code>"secondary_8.8.4.4"</code>
<code>MQTT_NOTIFICATION</code>			Object	Settings of MQTT notifications.	Yes	-
	<code>auth_enabled</code>		Literal	Enables or disables MQTT notifications on behalf of a specific user.	Yes	<code>true</code> means sending on behalf of the user is enabled; <code>false</code> means sending on behalf of the user is disabled
	<code>certificate_cert</code>		String	Client certificate that corresponds to the root certificate	Yes, if <code>"certs_enable": true</code>	Certificate in PEM format
	<code>certificate_key</code>		String	Client key that corresponds to the client certificate	Yes, if <code>"certs_enable": true</code>	Key in Base64 format
	<code>certificate_root</code>		String	Root certificate issued by a Certificate Authority.	Yes, if <code>"certs_enable": true</code>	Certificate in PEM format
	<code>certs_enabled</code>		Literal	Enables or disables the use of a secure TLS connection for MQTT notifications.	Yes	<code>true</code> : secure connection enabled; <code>false</code> : secure connection disabled
	<code>event_topic</code>		String	Name of the MQTT-topic for sending MQTT notifications.	Yes	MQTT-topic name
	<code>login</code>		String	User name.	Yes, if	User name.

				"auth_enabled": true	
	notifications_enabled	Literal	Enables or disables sending events via the MQTT protocol.	Yes	true: sending MQTT protocol enabled; false: sending over the protocol disabled
	password	String	User password	Yes, if "auth_enabled": true	Password that corresponds to user name
	server_address	String	MQTT broker IP address	Yes	String format: XXX.XXX.XXX example: "server_address": "192.168.1.1"
	server_port	Integer	MQTT broker port	Yes	You can use ports 1883 and 8883 to connect Kasp Secure Gateway to an MQTT broker residing in an internal network and ports 8884 and 8885 to connect to a broker residing on an external network
SYSLOG		Object	Syslog sending settings.	Yes	-
	certificate	String	Content of the security certificate for event forwarding over TCP/TLS		Certificate in PEM format
	enable	Literal	Enables or disables the use of a syslog server for event forwarding.		true: use a syslog server for event forwarding; false: do not use a syslog server for event forwarding
	host	String	IP address and port of the Syslog server		String format: XXX.XXX.XXX:XXXX example: "host": "192.168.1.1:514"
	mode	String	Event forwarding protocol		"tcp": forward via TCP; "udp": forward via UDP; "tcp+udp": forward via TCP using a TCP connection
	port	Integer	Syslog server port		Server port
TIME		Object	The current date and time.	Yes	-

			Read-only		
	<code>date</code>	String	Current date	No	Date formatted as "YYYY/MM/DD", example: "date" "2023/12/31"
	<code>time</code>	String	Current time	No	Time formatted as "HH:MM:SS", example: "time" "23:59:59"
UPDATE		Object	information about updates.	Yes	-
	<code>firmware_update_start</code>	Literal	Starting the Kaspersky IoT Secure Gateway 1000 update procedure.		<code>true</code> means a update will run; <code>false</code> is the default value.

Configuring industrial protocol traffic filtering

You can use the Kaspersky IoT Secure Gateway Network Protector application to configure rules for blocking and filtering industrial protocol traffic in the [Kaspersky IoT Secure Gateway 1000 configuration settings](#). Industrial traffic filtering uses packet analysis rules and includes the following checks:

- filtering of commands in the MQTT and Modbus protocols;
- Scanning for MQTT and Modbus traffic anomalies.

For Kaspersky IoT Secure Gateway Network Protector to work, you need to configure it first. When started without a completed configuration, Kaspersky IoT Secure Gateway 1000 [enters emergency mode](#), as it cannot receive traffic filtering rules to ensure a secure state.

To configure traffic filtering rules for industrial protocols:

1. Use Kaspersky Update Utility to download files with lists of supported network packet analysis rules:
 - The `industrial_commands.rules` file contains a list of supported command filtering rules for industrial protocols.
 - The `industrial_anomalies.rules` file contains a list of supported traffic anomaly detection rules for industrial protocols.

The identifier (sid) 90000001 is used for internal purposes and cannot be assigned to any rule.

For detailed information on using the utility, refer to the Kaspersky Update Utility documentation.

2. If required, select from these files the rules that you want to apply to industrial protocol traffic filtering.
3. Encode the lists of command filtering and anomaly detection rules as two separate Base64 strings.

4. [Stop](#) Kaspersky IoT Secure Gateway Network Protector if running.

While Kaspersky IoT Secure Gateway Network Protector is stopped, transit traffic on the device will be blocked to ensure the security of connected devices.

5. In the menu in the left part of the web interface screen, select **Settings** → **Configuration**.

6. In the configuration field under `kaspersky.kisg.netprotector`, add `"APP_CONFIGURATION": {}`.

7. Inside `APP_CONFIGURATION`, specify the following settings to enable and configure industrial protocol traffic filtering:

- Add an `"industrial_commands_rules": ""` parameter and specify a list of Base64-encoded rules for filtering commands at industrial protocol level.
- Add an `"industrial_anomaly_rules": ""` parameter and specify a list of Base64-encoded rules for detecting traffic anomalies at industrial protocol level.

As a result, the settings configuration under `kaspersky.kisg.netprotector` will appear as shown below:

```
"APP_CONFIGURATION": {  
  "industrial_commands_rules": " <Base64 encoded rules> ",  
  "industrial_anomaly_rules": " <Base64-encoded rules> "  
}
```

For Kaspersky IoT Secure Gateway Network Protector to work, define at least one configuration setting, or else Kaspersky IoT Secure Gateway 1000 [will enter emergency mode](#) after you start it, as it cannot receive traffic filtering rules to ensure a secure state. You can disable only one of the settings by putting empty quotation marks `""` as the parameter value.

After adding `APP_CONFIGURATION` and its settings, you cannot delete it, as it is required for the application to work.

8. Click **Save** to apply the configuration settings.

9. [Start](#) Kaspersky IoT Secure Gateway Network Protector.

Industrial protocol traffic will be filtered using the specified rules. If the rule is triggered, traffic that matches the rule is blocked, and the IP address where the traffic originated is added to the IP address denylist. The information that the IP address was blocked is sent to the Kaspersky IoT Secure Gateway 1000 firewall. The traffic blocking event is recorded in the [audit log](#).

Changing the language of the Kaspersky IoT Secure Gateway 1000 web interface

Kaspersky IoT Secure Gateway 1000 lets you select the language of the web interface.

To change the language of the Kaspersky IoT Secure Gateway 1000 web interface:

1. In the menu in the left part of the web interface page, select  **<user name>**.

The user menu opens.

2. Under **Language** in the user menu, select **Russian** or **English**.

The Kaspersky IoT Secure Gateway 1000 web interface language will be changed to the language you selected.

You can also change the web interface language on the Kaspersky IoT Secure Gateway 1000 login page or on the page for resuming a connection session with Kaspersky IoT Secure Gateway 1000, in the upper part of the page on the right.

Performing common tasks

This section contains a description of the common user tasks and instructions on how to perform them.

Monitoring the state of Kaspersky IoT Secure Gateway 1000

Summary information about the status of Kaspersky IoT Secure Gateway 1000 and the device running Kaspersky IoT Secure Gateway 1000 is displayed in the **Status** section. This section contains the following information blocks:

- Device details, such as [the name](#), IP address and ID, and the version of Kaspersky IoT Secure Gateway 1000 installed on the device.
- The type of network device elected [when Kaspersky IoT Secure Gateway 1000 was installed](#) on the device. One of the following types is possible:
 - *Network router*. This device type enables the transmission of network packets over the IP in both directions: from the gateway and to the gateway.
A policy is applied to the network router that ensures routing of the traffic that flows through the device.
 - *Unidirectional gateway*. This device type enables the transmission of network packets over the IP in one direction and does not allow transmission in the opposite direction.
Unidirectional gateway applies a policy to ensure that devices on the LAN transmit data to the WAN, whereas local resources are not exposed to any impact from the WAN.
- Kaspersky Security Center Administration Server connection status.
- Links to articles in the Kaspersky IoT Secure Gateway 1000 online help.

Monitoring the state of a cellular connection

If the device does not have a modem, the cellular connection is unavailable and modem settings are hidden.

This functionality is available to the [administrator](#) only.

To use the modem as the main communication channel, [enable the use of a cellular connection](#).

You can track the state of the Kaspersky IoT Secure Gateway 1000 cellular connection under **Network** → **WAN**. The **Modem settings** section displays the following information about the cellular connection status:

- **Modem status** – displays the state of the Kaspersky IoT Secure Gateway 1000 cellular connection. The following values are available for this setting:
 - **Connected**: the modem is connected to the device and a connection between the modem and the carrier is established.

- **Not available:** the modem is connected to the device, but there is no connection between the modem and the carrier.
- **Signal quality** – the quality of the cellular connection. The number of lines shows the signal level of the cellular network that the device running Kaspersky IoT Secure Gateway 1000 is connected to. As the signal quality decreases, the number of bars is reduced.

In the **Modem DNS server addresses** section, the information about the IP addresses of the primary and secondary DNS servers of the modem is displayed. The **Profiles** table displays information about the available [modem profiles](#).

If there is no cellular connection, you must verify that the following conditions are met:

- The SIM card used in the modem is valid and has an active plan that supports an Internet connection through the modem.
- The selected modem profile matches the SIM card being used.
- The modem is available for use (a **Connected** status is displayed).

If the modem is not available for use (a **Not available** status is displayed), [reboot Kaspersky IoT Secure Gateway 1000](#) and check modem availability once again. Devices that access the Internet through Kaspersky IoT Secure Gateway 1000 must obtain the internal network settings through the DHCP server of Kaspersky IoT Secure Gateway 1000. The relevant addresses of DNS servers from cellular network providers will be received together with these settings.

Monitoring Kaspersky IoT Secure Gateway 1000 audit events

This section contains instructions on monitoring events that are registered in Kaspersky IoT Secure Gateway 1000.

An *audit event* is a record containing information about the detection of data in the system or internal network that requires the attention of an employee responsible for information security in your organization. Audit events are stored in the memory of the Kraftway Rubezh-N embedded computer.

Kaspersky IoT Secure Gateway 1000 logs the following event types:

- Firewall audit events, such as events from Kaspersky IoT Secure Gateway Network Protector. You can view these in [the event log](#) in the **Events** section.
- Operating system audit events. You can view these in the [audit log](#) in the **Audit** section.

You can also view firewall and operating system audit events [from the Kaspersky Security Center 14.2 Web Console](#). If necessary, you can also [configure forwarding of the event log to a Syslog server](#) or [configure forwarding of MQTT notifications regarding event registration](#).

Monitoring firewall audit events

This section contains instructions on monitoring firewall audit events logged by Kaspersky IoT Secure Gateway 1000, such as those registered by the Kaspersky IoT Secure Gateway Network Protector application.

About firewall audit events


The table below describes firewall audit events logged by Kaspersky IoT Secure Gateway 1000 and the Kaspersky IoT Secure Gateway Network Protector application.

Firewall audit events

Event name	Event text	Severity	Subject ID
Audit: Audit subsystem start	Audit subsystem is running	Informational	System: Audit
admin: Log export user: Log export	The log is exported	Informational	Administrator or user
admin: Log export error user: Log export error	Failed to export the log	Warning	Administrator or user
Audit: Audit log overwrite	Audit log is overwritten due to full storage	Informational	System: Audit
Audit: Audit log is running out of space	The audit log will be overwritten after <number or entries>	Warning	System: Audit
TrafficController: Traffic blocking	The traffic from the device <IP address> is blocked	Warning	System: TrafficController
TrafficController: Rule creation limit for IDSPProxy	Failed to block device <IP address>: maximum limit on blocking rules reached(<maximum number of rules>)	Critical	System: TrafficController
TrafficController: Changing the configuration of firewall rules	Configuration of the firewall rules is changed	Informational	System: TrafficController
KscController: Changing the application routes	Application routes are changed	Informational	System: KscController
Launcher: Switching Kaspersky IoT Secure Gateway Network Protector to emergency mode	Emergency mode activated for Kaspersky IoT Secure Gateway Network Protector application	Critical	System: Launcher
Audit: Audit subsystem test message	The test message was successfully recorded during audit subsystem diagnostics	Informational	System: Audit
TrafficController: Error creating route	User-defined route not applied: <description>	Warning	System: TrafficController

Viewing the firewall audit log

Kaspersky IoT Secure Gateway 1000 logs firewall audit events, such as those registered by the Kaspersky IoT Secure Gateway Network Protector application.

When a critical event occurs, an exclamation mark  *alarm icon* is displayed next to the **Events** menu section on the left. In that event, contact the employee responsible for information security in your organization.

To view the firewall audit log:

1. In the menu in the left part of the web interface page, select the **Events** section.




This opens the **Events** page, which contains a table of all registered firewall audit events. Events in the table are refreshed every 30 seconds. New events are displayed at the top. The table can display up to 1024 of the last registered events. If the number of events is exceeded, the log is overwritten starting with the oldest entries.

If the audit event language in the table does not match the system language, [select the relevant web interface language in the menu](#) and refresh the page to apply the changes.

The following information is displayed for each log entry:

- **Date and time** – date and time when the event was registered.
- **Event name**: name of the registered event.
- **Event text**: detailed information about the registered event, such as modification of firewall settings.
- **Subject ID**: source of the registered event:
 - **Administrator**: the event was triggered by an administrator action in the system.
 - **User**: the event was triggered by a user action in the system.
 - **System**: the event was triggered by a system action. For each event, the log displays the name of the subsystem where the event occurred.
- **Severity**: the severity level of the registered event.

Events are categorized by the following severity levels:

-  – *Informational*. Informational events contain reference information. These events usually do not require an immediate response.
-  – *Warning*. Warning events contain information that requires attention. These events may require a response.
-  – *Critical*. Critical events contain information that may have a critical impact on the security of the network in which Kaspersky IoT Secure Gateway 1000 resides. These events require an immediate response. Critical events in the table are highlighted in red.

2. To view events for a specific date or period, click in the **Date** field, select a specific date or start and end dates for the period, and click **Apply**.

The table will display events for the selected date or period.

3. To view events that have a specific severity, select the relevant severity level from the **Severity** drop-down list in the upper part of the table and click **Apply**. You can select one or multiple values. Events with all severity levels are displayed by default.

The table will display events with the selected severity level.

4. To view events that came from specific sources, select the relevant subject from the **Subject ID** drop-down list in the upper part of the table and click **Apply**. You can select one or multiple values. All registered events are displayed by default.

The table will display events from the selected sources.

- If you need to clear all the set filters for displaying events in the table, click **Reset all**.
All registered events will be displayed in the table.
- To display older events, click **Load more** under the table.

The **Load more** button is always available, even if there are no earlier events.

Exporting the firewall audit log

You can save the firewall audit log on the local computer.

To save the firewall audit log on the local computer:

- In the menu in the left part of the web interface page, select the **Events** section.
This opens the **Events** page, which contains a table of all registered firewall audit events.
- Click **Download log**.
- In the opened window, specify the path for saving the event log file on the local computer, specify its name if necessary, and save the file.

The firewall audit log will be saved on the local computer in CSV format. If you [applied filters](#) in the audit events table before saving the log, it will display filtered events only.

Monitoring operating system audit events

This section contains instructions on monitoring operating system audit events.

This functionality is available to the [administrator](#) only.

About operating system audit events

The table below describes operating system audit events registered by Kaspersky IoT Secure Gateway 1000.

Operating system audit events

Event name	Event text	Severity	Subject ID
Audit: Audit subsystem start	Audit subsystem is running	Informational	System: Audit
Audit: Audit subsystem test message	The test message was successfully recorded during audit subsystem diagnostics	Informational	System: Audit
admin: Log export	The log is exported	Informational	Administrator

admin: Log export error	Failed to export the log	Warning	Administrator
Audit: Audit log overwrite	Audit log is overwritten due to full storage	Informational	System: Audit
Audit: Audit log is running out of space	The audit log will be overwritten after <number or entries>	Warning	System: Audit
KscController: Rebooting the device	The device is being rebooted	Informational	System: KscController
KscController: Uploading the application certificate	Application certificate is uploaded to the certificate storage	Informational	System: KscController
Launcher: Attempting to launch an incompatible version of the application	An attempt to launch the application version incompatible with the system was detected	Warning	System: Launcher
Launcher: Attempting to launch a blocked application	An attempt to run a blocked application is detected	Warning	System: Launcher
Launcher: Launching an application	The application <application name> was started	Informational	System: Launcher
Launcher: Error launching an application	Failed to start the application <application name>	Warning	System: Launcher
Launcher: Untrusted application	Failed to verify the integrity of the application <application name>	Critical	System: Launcher
Launcher: Stopping an application	The application <application name> was stopped	Informational	System: Launcher
Launcher: Application has failed	The application <application name> failed with an error	Warning	System: Launcher
Launcher: Changing application autorun	The list of applications for autorun is changed	Informational	System: Launcher
Launcher: Error changing application autorun	Failed to change the list of applications for autorun	Warning	System: Launcher
Launcher: Enabling the non-immune mode	The device is running in non-immune mode; immunity is not guaranteed	Warning	System: Launcher
Launcher: Enabling the developer mode	The device is running in developer mode	Warning	System: Launcher
Launcher: Attempting to download a new version of the application	An attempt to download a new version of an installed application is detected.	Critical	System: Launcher
Orchestrator: Downloading the application	Download of the application <application name> was started	Informational	System: Orchestrator
Orchestrator: Successful application download	The application <application name> was successfully downloaded to device	Informational	System: Orchestrator
Orchestrator: Successful application	The application <application name> was successfully installed	Informational	System: Orchestrator

installation			
Orchestrator: Uninstalling the application	Uninstallation of the application <application name> was started	Informational	System: Orchestrator
Orchestrator: Successful application uninstallation	<application name> was successfully uninstalled	Informational	System: Orchestrator
Orchestrator: Application download error	Failed to download the application <application name>	Warning	System: Orchestrator
Orchestrator: Application signature verification error	Failed to verify authenticity of the <application name> application signature	Critical	System: Orchestrator
Orchestrator: Application installation error	Failed to install the application <application name>	Warning	System: Orchestrator
Orchestrator: Application installation error	Failed to install the application <application name>. You have reached the limit on the number of applications that can be installed on the device.	Warning	System: Orchestrator
Orchestrator: Application uninstallation error	Failed to uninstall the application <application name>	Warning	System: Orchestrator
TrafficController: Enabling a network cluster	The network cluster is enabled and its settings are configured	Warning	System: TrafficController
TrafficController: Disabling a network cluster	The network cluster is disabled	Warning	System: TrafficController
EmergencyManager: Enabling the Emergency support mode	A critical operating system error is detected. Emergency support mode is enabled: <description>	Critical	System: EmergencyManager
EmergencyManager: Limiting the operating system functions	Operating system functions (<description>) are limited as emergency support mode is active	Critical	System: EmergencyManager
BlobContainer: Component blocked from starting	Starting <component> with integrity violation blocked	Critical	System: BlobContainer
Updater: System update	Full system update is started	Informational	System: Updater
Updater: Verifying updates	Downloaded updates are verified and ready to install	Informational	System: Updater
Updater: Downloading updates	Updates downloaded successfully	Informational	System: Updater
Updater: System update successful	System update completed successfully	Informational	System: Updater
Updater: No update required	No update required. The latest system version is installed	Informational	System: Updater
Updater: System update	Error <description> occurred during	Critical	System: Updater


error	system update		
Updater: Error downloading updates	Failed to download updates	Informational	System: Updater
Updater: Error rebooting the device	Failed to restart the device while installing updates	Critical	System: Updater
Updater: Invalid updates	Downloaded updates are invalid and cannot be installed	Warning	System: Updater
admin: Date and time change	System date and time were changed manually	Informational	Administrator
KscController: Time synchronization with the source	System time is synchronized with Kaspersky Security Center	Informational	System: KscController
admin: Account credentials expiry user: Account credentials expiry	User name and password expire in <number of days> days	Informational	Administrator or user
admin: Certificate expiry user: Certificate expiry	User certificate expires in <number of days> days	Informational	Administrator or user
admin: User account credentials expired user: User account credentials expired	User name and password expired, refresh the account credentials	Warning	Administrator or user
admin: User certificate expired user: User certificate expired	User certificate has expired	Warning	Administrator or user
Authenticator: User blocked	User blocked due to exceeding the number of failed login attempts	Critical	System: Authenticator
WebServer: Connection session lock	Connection session blocked due to inactivity	Informational	System: WebServer
admin: Modified lockout duration after failed password entry attempts user: Modified lockout duration after failed password entry attempts	Lockout duration after failed password attempts changed. New value: <new value> minutes	Informational	Administrator or user
admin: Modified user idle time before locking user: Modified user idle time before locking	User idle time before locking changed, new value: <new value> min	Informational	Administrator or user
admin: Modified maximum number of failed login attempts user: Modified maximum number of failed login attempts	Maximum number of failed login attempts changed. New value: <new value>	Informational	Administrator or user

admin: Change credentials user: Change credentials	The administrator password for initial login is changed	Informational	Administrator or user
admin: Change credentials user: Change credentials	Password for user <user name> changed	Informational	Administrator or user
admin: Change credentials user: Change credentials	Certificate for user <user name> changed	Informational	Administrator or user
admin: Change credentials user: Change credentials	<user name> user name changed	Informational	Administrator or user
admin: Creating a user account	User account created for <user name>	Informational	Administrator
admin: Error creating user account	User account for <user name> already exists	Warning	Administrator
admin: Deleting a user account	User account for <user name> deleted	Informational	Administrator
admin: User authentication user: User authentication	<user name> logged in	Informational	Administrator or user
Authenticator: User authentication error	User <user name> authentication error: incorrect password	Warning	System: Authenticator
Authenticator: User authentication error	User <user name> authentication error: invalid certificate	Warning	System: Authenticator
Authenticator: User authentication error	User <user name> authentication error: no user found with specified name	Warning	System: Authenticator
admin: Restoring the system configuration	Status of the operating system configuration restoring from the backup: <status>	Informational	Administrator
admin: Backing up the system configuration	Status of the backup creation from the operating system configuration: <status>	Informational	Administrator
admin: Generation of the integrity check report	Generation of the integrity check report started: <description>	Informational	Administrator
IntegrityService: Integrity check status	Integrity check status: <status>	Informational	System: IntegrityService
IntegrityService: Object integrity violation	<object> integrity violated: <description>	Critical	System: IntegrityService
admin: Operating system self-testing start	Operating system self-testing started	Informational	Administrator

SelfTestManager: Operating system error during self-testing	Operating system error during self-testing detected: <description>	Critical	System: SelfTestManager
SelfTestManager: Operating system self-testing result	Operating system self-testing result: completed successfully	Informational	System: SelfTestManager
SelfTestManager: Operating system self-testing result	Operating system self-testing result: errors detected	Informational	System: SelfTestManager
SelfTestManager: Operating system self-testing result	Operating system self-testing result: canceled manually	Informational	System: SelfTestManager

Viewing the operating system audit log

Kaspersky IoT Secure Gateway 1000 saves events related to system security to the operating system audit log. These events are created by [system entities](#). Each event contains the identifier (user or component name) of the subject that registered the event.

When a critical event occurs, an exclamation mark  is displayed next to the **Audit** menu section on the left. In that event, contact the employee responsible for information security in your organization.

To view the operating system audit log:

1. In the menu in the left part of the web interface page, select the **Audit** section.

This opens the **Audit** page, which contains a table of all registered operating system audit events. Events in the table are refreshed every 30 seconds and displayed in reverse chronological order (new events first). The table can display a maximum of 1024 of the last registered events. If the number of events is exceeded, the log is overwritten starting with the oldest entries.




If the audit event language in the table does not match the system language, [select the relevant web interface language in the menu](#) and refresh the page to apply the changes.


The following information is displayed for each log entry:

- **Date and time** – date and time when the event was registered.
- **Event name**: name of the registered event.
- **Event text**: detailed information about the registered event.
- **Subject ID**: source of the registered event:
 - **Administrator**: the event was triggered by an administrator action in the system.
 - **User**: the event was triggered by a user action in the system.
 - **System**: the event was triggered by a system action. For each event, the log displays the name of the subsystem where the event occurred.

- **Severity:** the severity level of the registered event.

Events are categorized by the following severity levels:

-  – *Informational.* Informational events contain reference information. These events usually do not require an immediate response.
-  – *Warning.* Warning events contain information that requires attention. These events may require a response.
-  – *Critical.* Critical events contain information that may have a critical impact on system operation. These events require an immediate response.

When a critical event occurs, an exclamation mark  *alarm icon* is displayed next to the **Audit** menu section on the left. In the table, audit events with a critical level of severity are highlighted in red.

2. To view events for a specific date or period, click in the **Date** field, select a specific date or start and end dates for the period, and click **Apply**.

The table will display events for the selected date or period.

3. To view events that have a specific severity, select the relevant severity level from the **Severity** drop-down list in the upper part of the table and click **Apply**. You can select one or multiple values. Events with all severity levels are displayed by default.

The table will display events with the selected severity level.

4. To view events that came from specific sources, select the relevant subject from the **Subject ID** drop-down list in the upper part of the table and click **Apply**. You can select one or multiple values. All registered events are displayed by default.

The table will display events from the selected sources.

5. If you need to clear all the set filters for displaying events in the table, click **Reset all**.

All registered events will be displayed in the table.

6. To display older events, click **Load more** under the table.

The **Load more** button is always available, even if there are no earlier events.

Exporting the system audit log

You can save the operating system audit log on the local computer.

To save the operating system audit log on the local computer:

1. In the menu in the left part of the web interface page, select the **Audit** section.
This opens the **Audit** page, which contains a table of all registered operating system audit events.
2. Click **Download log**.
3. In the opened window, specify the path for saving the audit log file on the local computer, specify its name if necessary, and save the file.

The operating system audit log will be saved on the local computer in CSV format. If you [applied filters](#) in the audit events table before saving the log, it will display filtered events only.

Viewing events when connected to Kaspersky IoT Secure Gateway 1000 via the console port

Kaspersky IoT Secure Gateway 1000 lets you view Kaspersky IoT Secure Gateway 1000 event logs in real time. To do this, connect the Kraftway Rubezh-N embedded computer to a local computer through the console port.

A *console port* is a control port providing out-of-band access to the embedded computer.

To view Kaspersky IoT Secure Gateway 1000 event logs in real time via a console port connection:

1. Use a console cable with RJ-45 DB-9 / RS-232 connectors to connect the port on the front panel of the Kraftway Rubezh-N embedded computer to a computer or laptop.

If your computer does not have a port for the corresponding cable, you can use a USB-COM adapter.

2. [Turn on the embedded computer.](#)

3. Using a terminal emulator on the local computer, connect to the embedded computer.

Before connecting, please specify the following connection settings in your terminal emulator:

- The data transfer rate should be 115,200 baud, or a different value if it is specifically set for the **Recovery mode** parameter
- The number of data bits, availability and type of the parity bit, and the number of stop bits should be 8n1
- Hardware flow control

Kaspersky IoT Secure Gateway 1000 events will be displayed in real time in the interface of the terminal emulation program running on the desktop or laptop.

Exporting the system log

You can save the system log containing diagnostic information about Kaspersky IoT Secure Gateway 1000 operation on the local computer. You can use this log to troubleshoot possible system issues.

This functionality is available to the [administrator](#) only.

To save the system log on the local computer:

1. In the menu on the left side of the screen, select **Settings** → **Diagnostics**.

2. Click **Save to file**.

3. In the window that opens, select a path for saving the event log file on the local computer, provide a new name if required, and save the file.

The system log will be saved on the local computer. By default, the file is saved with the name log_files.tar.gz.

Managing apps

Application management is available to the [administrator](#) only. Users can only view the list of applications and the list of application logs.

All applications available to install are displayed in the Kaspersky IoT Secure Gateway 1000 web interface, under **Applications** → **All apps**. Applications in the **All apps** table are sorted by name by default. You can click a column header to sort the table by that column.

For each application, the following information is displayed on the **All apps** tab.

- **Name** – the name of the application and its icon. You can view detailed information about the application and its developer, the Privacy Policy and the Application License Agreement by clicking the name of the application in the table.
- **Title** – a brief description of the application.
- **Version** – the number of the last application version available for installation.
- **Size** – the size of the application installation package.
- **Category** – categories the app belongs to.
- **Publication** date – the date when the last application version was published.
- **Status** – application installation status (error installing or uninstalling if installation failed) If the security of an application is compromised, a **Compromised** status is displayed for that application. A compromised application cannot be installed.
- **Control** – the button for [installing an application](#) if the application is available for installation, or the installation status.

All installed applications are displayed in the Kaspersky IoT Secure Gateway 1000 web interface, under **Applications** → **Installed apps**. Applications in the **Installed apps** table are sorted by name by default. You can click a column header to sort the table by that column.

For each installed application the following information is displayed on the **Installed apps** tab.

- **Name** – the name of the application and its icon. You can view detailed information about the application and its developer, the Privacy Policy and the Application License Agreement by clicking the name of the application in the table.
- **Issuer** – the name of the company that released the application.
- **Version** – the installed version of the application.
- **Application type** – the type of the application based on its function in Kaspersky IoT Secure Gateway 1000.
- **Start rule** – the [method used to start the application](#) on the device: autorun, manual start, or blocking. You can configure a start rule only for configured applications that have the **Run** or **Stopped** status.
- **Manifest** – application configuration file. To view the contents of the manifest, click **View**.

- **Status** – the application operation status (running or stopped). If the application is not configured or is configured incorrectly, the status is **Pending**. In this case, configure the application, for example, [in Kaspersky Security Center 14.2 Web Console](#).
- **Control** – the button to [start or stop](#) the application.
- **Uninstall** – the button for [uninstalling an application](#)

Downloading and installing apps

You can download and install no more than 20 apps in Kaspersky IoT Secure Gateway 1000.

To download and install an app in Kaspersky IoT Secure Gateway 1000, do as follows:

1. In the menu in the left part of the screen, select **Applications** → **All apps**.
A table of all applications that are available to install will be displayed.
2. To manually update the application list in the table, click the **Reload table** button at the top of the page.
3. To sort the applications in the table, click the column header by which you want to sort.
By default, the applications are sorted alphabetically by name.
4. To view detailed information about an application before installation, click the application name.
A window opens with the detailed information about the application.
5. Click the **Install** button in the **Action** column next to the application you want to install in Kaspersky IoT Secure Gateway 1000.

All available apps are guaranteed to work for the [unidirectional gateway network device type](#). Only the Kaspersky IoT Secure Gateway Network Protector and Kaspersky Debug Service applications are guaranteed to work for the [network router device type](#). You can install other applications, but they are not guaranteed to work on the device.

The application is downloaded and installed in Kaspersky IoT Secure Gateway 1000. Information about downloading and installing the application is saved in the [system audit log](#). The installed application appears under **Applications** → **Installed apps**. In this section, you can [start or stop the application](#), [manage its startup rules](#), and [delete the application](#).

Installed applications are not updated automatically. To update an application, first [uninstall the currently installed version of the application](#) and then install the new version. If you remove a delisted (not displayed on the **All apps** tab) version of an application, you cannot revert to that version later.

Starting and stopping apps

You can start and stop applications in the Kaspersky IoT Secure Gateway 1000 web interface.

To start an application on a device:

1. In the menu in the left part of the screen, select **Applications** → **Installed apps**.

A table of all applications installed in Kaspersky IoT Secure Gateway 1000 is displayed.

2. To sort the applications in the table, click the column header by which you want to sort.

By default, the applications are sorted alphabetically by name.

3. In the row of the application that you want to start, click the **Start** button in the **Manage** column.

You can start the application in the following cases:

- The application is installed and configured without errors and has a **Stopped** status.
- The **Manual start** or the **Autostart** rule is selected for the application.

The applications in the **Pending** status must first be [configured in Kaspersky Security Center 14.2 Web Console](#). Wait for the **Stopped** status to appear.

The application is started, and the corresponding status is displayed in the table. Information about the application startup is saved in the [operating system audit log](#).

If the application cannot be started, an **Error** status is displayed. In this case, [uninstall the application](#) and [install it again](#).

To stop an application on a device:

1. In the menu in the left part of the screen, select the **Applications** section and select the **Installed apps** tab.

A table of all applications installed in Kaspersky IoT Secure Gateway 1000 is displayed.

2. To sort the applications in the table, click the column header by which you want to sort.

By default, the applications are sorted alphabetically by name.

3. In the row of the application that you want to stop, click the **Stop** button in the **Manage** column.

You can stop the application if configured without errors and has a **Run** status.

The application is stopped, and the corresponding status is displayed in the table. Information about the application being stopped is saved in the [operating system audit log](#).

Managing application launch rules

You can use the Kaspersky IoT Secure Gateway 1000 web interface to configure how the application starts in Kaspersky IoT Secure Gateway 1000 (automatically or manually) or prevent the application from starting.

To configure the application start rules:

1. In the menu in the left part of the screen, select **Applications** → **Installed apps**.

A table of all applications installed in Kaspersky IoT Secure Gateway 1000 is displayed.

2. To sort the applications in the table, click the column header by which you want to sort.

By default, the applications are sorted alphabetically by name.

3. In the row of the application for which you want to configure a start rule, in the **Start rule** column, select one of the following values from the drop-down list:

- **Autostart** – the application starts automatically when Kaspersky IoT Secure Gateway 1000 is turned on or restarted.

You can manually [stop and start](#) the application if necessary.

- **Manual start** – the application starts only [manually](#) by clicking the **Start** button.

By default, the manual start rule is applied to the application after it is installed.

- **Block start** – the application is not available to start. The **Run** button is not available.

If you have changed the launch rule for a running application, the modified launch rule will be applied only after the application is stopped. You can [stop the application manually](#) to apply the start rule.

Applications in the **Pending** status need to first be [configured through the Kaspersky Security Center 14.2 Web Console](#). Then you need to wait for the **Run** or **Stopped** status to appear.

The start rule is applied to the selected application in Kaspersky IoT Secure Gateway 1000. Information about changes to the list of start rules is saved in [the system audit log](#).

You can also manage application start rules from the Kaspersky Security Center 14.2 Web Console.

Removing apps

You can uninstall applications from the Kaspersky IoT Secure Gateway 1000 web interface.


To remove an application:

1. In the menu in the left part of the screen, select **Applications** → **Installed apps**.

A table of all applications installed in Kaspersky IoT Secure Gateway 1000 is displayed.

2. To sort the applications in the table, click the column header by which you want to sort.

By default, the applications are sorted alphabetically by name.

3. In the row of the application you want to remove, click the trash bin icon  in the **Delete** column and confirm the deletion in the window that opens.

The application and its configuration, log, and files are removed from Kaspersky IoT Secure Gateway 1000. The application is removed from the table of installed applications. Information about application removal is saved to the [operating system audit log](#).

If you remove a delisted (not displayed on the **All Apps** tab) version of an application, you cannot reinstall that version later.

If an error occurs during removal, the **Status** column will show an **Error** status; you will be unable to start or stop the application, configure a start rule, or view the manifest. In that event, you have to [reinstall the application](#).

The routes configured in Kaspersky Security Center 14.2 Web Console and associated with the removed application stop working (their status changes to **Error**). It is recommended to [reconfigure the routes](#) associated with the removed applications in Kaspersky Security Center 14.2 Web Console.

Monitoring the state of apps

Kaspersky IoT Secure Gateway 1000 logs events generated by installed applications.

For each app, the logs are stored as the log_files_<app_id>.tar.gz archive. The archive contains no more than five log files in the LOG format, no more than 10 MB each (the maximum archive size is 50 MB). When the maximum size of the files stored in the archive is reached, Kaspersky IoT Secure Gateway 1000 deletes the oldest file, and the new events are logged to a new file.

Kaspersky IoT Secure Gateway 1000 ensures the safety of the app logs when the system is restarted, turned off, or updated. When the app is uninstalled or updated, Kaspersky IoT Secure Gateway 1000 deletes the log of this application.

To save the application log on the local computer:

1. In the web interface menu, select the **Applications** section and the **Application log** tab.
2. To update the app logs table, click the **Reload table** button at the top of the page.
3. On the page that opens, click **Download** next to the desired application in the **Log** column. For the logs available for download, their size is displayed.
4. In the window that opens, specify a path, provide a file name if required, and save the file.

The app log log_files_<app_id>.tar.gz is saved on the local computer to the default download folder (for example, to the browser downloads folder).

Until the app log is fully downloaded, you cannot download the log of another app (the **Download** button is not available). If there are no logged events for the app yet, the log is not available for download, and the corresponding status is displayed in the **Log** column.

Self-testing and integrity control in Kaspersky IoT Secure Gateway 1000

This functionality is available to the [administrator](#) only.

Self-testing

Kaspersky IoT Secure Gateway 1000 self-testing is a process that monitors the performance of the KasperskyOS security features and overlaid protection tools.

The self-testing system performs diagnostics of the following functions:

- Audit
- User identification and authentication tool
- Network traffic blocking tool
- Kaspersky IoT Secure Gateway Network Protector application

To start self-testing, do as follows:

1. In the menu on the left side of the screen, select the **Self-diagnostics** section.
2. In the **Self-testing** subsection, click **Start testing**.

The self-testing results for each feature are displayed in the **Self-testing** table, and the overall testing status is displayed next to the **Start testing** button. If errors occur during self-testing, Kaspersky IoT Secure Gateway 1000 switches to [emergency support mode](#).

Start events and self-testing results are recorded in the [system audit log](#).

Integrity control

Integrity control checks system and user application files and data through electronic signature (checksum) verification.

Kaspersky IoT Secure Gateway 1000 provides two types of integrity checks: automatic and manual.

An automatic check is performed when Kaspersky IoT Secure Gateway 1000 starts and checks the user application checksums. If the integrity of user applications is compromised, Kaspersky IoT Secure Gateway 1000 records information about the integrity violation in the audit log and automatically switches to [emergency support mode](#).

A manual integrity check can be started by the administrator only.

To start an integrity check manually and view the results, do as follows:

1. In the menu on the left side of the screen, select the **Self-diagnostics** section.
2. In the **Integrity check** subsection, click **Start check**.

The application generates a report file after the integrity check is completed. The status, date and time of the last manual integrity check are displayed next to the **Download report** button.

3. Click **Download report** to save the report file containing the manual integrity check results in TXT format to the local computer.

In the event that the manual check detects an integrity violation, the application does not automatically switch to emergency support mode. The administrator has to read the report and decide on a further course of action.

The manual integrity check report file consists of a report header and a report body. The report file header contains the following information:

- Host ID

- Report generation date and time
- Name of the function for calculating the checksum for the report file
- Checksum of the report file
- Separator between the report header and the report body

The report body consists of the lines with the check status for each file participating in the integrity check procedure. Each line consists of the following fields, separated by the |:

- Path and name of the scanned file
- Date and time of the integrity check
- Name of the function for calculating the checksum
- Reference checksum for the file
- Calculated checksum for the file
- Integrity check status Possible statuses:
 - *File integrity verified successfully* – the reference and calculated checksums match. Any status other than this one may indicate a potential integrity violation, and the administrator is advised to analyze the incident.
 - *File content changed against reference!* – the calculated checksum differs from the reference one.
 - *File isn't present in integrity database!* – a file is detected that is not under integrity control. In this case, the reference checksum field is filled in with zeros.
 - *The file under integrity control was deleted or moved!* – the file under integrity control has been moved or deleted. In this case, the calculated checksum field is filled in with zeros.
 - *Package integrity violation!* – the file that contains the reference checksums of the files is corrupted or missing.

The following executable files and libraries must pass the integrity check:

- System libraries in the /lib folder
- System image file /loader_active/image.fit
- Local web interface files:
 - Files in the html/assets folder
 - Files in the html/css folder
 - Files in the html/js folder
 - Files authorization.html, index.html, troubleshooting.html
- System digital certificates:
 - File 3520p1.der (for the release version of the system)

- File 3020d1.der (for the developer version of the system)
- Files for working with applications:
 - Container file /packages/helpers/container
 - Application validation files in the /packages/schema folder

For these files and libraries, the report must show the "File integrity verified successfully" status, indicating that their code has not been changed and their checksum matches the reference one.

For the rest of the files, you need to analyze on your own, whether the changes are acceptable.

Backing up and restoring from a backup copy

Kaspersky IoT Secure Gateway 1000 has a backup and restore function designed to restore the system operating status in case of failures. Backup and restore are available to the administrator.

Valid backup and restoring of the settings of MQTT broker, web server or additional applications installed on Kaspersky IoT Secure Gateway 1000 are not guaranteed.

This functionality is available to the [administrator](#) only.

Creating a configuration backup

To create a configuration backup:

1. In the menu in the left part of the screen, select **Settings** → **Backup and recovery**.
2. In the **Backup** subsection, click **Create new file**.
3. Wait for the configuration backup to complete.
4. Click **Save file**.
5. In the window that opens, select the folder to store the backup copy and save the file.

Restoring configuration

Note: Configuration can be properly restored only if the version of Kaspersky IoT Secure Gateway 1000 from which the backup copy was created matches the version of Kaspersky IoT Secure Gateway 1000 to which the restore is being performed.

To restore a device configuration from a backup:

1. In the menu in the left part of the screen, select **Settings** → **Backup and recovery**.

2. In the **System restore** subsection, click **Select file**.
3. In the window that opens, select a backup file and open it.
4. Wait for the restore operation to complete.

If the configuration is restored successfully, the device is restarted.

Updating Kaspersky IoT Secure Gateway 1000

You can run a full Kaspersky IoT Secure Gateway 1000 update on the device through the web interface.

The system can be updated only if Kaspersky IoT Secure Gateway 1000 is connected to Kaspersky Security Center. A full update of Kaspersky IoT Secure Gateway 1000 from Kaspersky update servers is available only for version 3.0.

This functionality is available to the [administrator](#) only.

After Kaspersky IoT Secure Gateway 1000 is updated, the device will be restarted.

To run a full update of Kaspersky IoT Secure Gateway 1000, do as follows:

1. In the menu in the left part of the web interface page, select **Settings** → **Update**.
2. Click **Run update**.

This starts a check for available Kaspersky IoT Secure Gateway 1000 updates. If an update is found, it is downloaded, and a full update of Kaspersky IoT Secure Gateway 1000 is performed on the device. The device will be restarted during the update process.

Information about successfully found and downloaded updates and the Kaspersky IoT Secure Gateway 1000 update process is recorded in the [system audit log](#).

Restarting Kaspersky IoT Secure Gateway 1000

This functionality is available to the [administrator](#) only.

To restart Kaspersky IoT Secure Gateway 1000:

1. In the menu in the left part of the web interface page, select **Settings** → **Commands**.
2. Click **Restart device** and confirm deletion.

The device running Kaspersky IoT Secure Gateway 1000 will be restarted. The connection Kaspersky Security Center and Kaspersky IoT Secure Gateway 1000 will be unavailable while the device is restarting

Managing the system with the Kaspersky Security Center 14.2 Web Console

The Kaspersky Security Center 14.2 Web Console (the "Web Console") is a web application designed for centralized management and maintenance of an enterprise network security system. The Web Console is a Kaspersky Security Center 14.2 entity that provides a user interface. For detailed information about the Kaspersky Security Center 14.2 Web Console, please refer to the Kaspersky Security Center 14.2 Online Help Guide.

Kaspersky Security Center 14.2 and Kaspersky Security Center 14.2 Web Console are not included in the [Kaspersky IoT Secure Gateway 1000 distribution kit](#). They must be installed separately.

You can use the Kaspersky Security Center 14.2 Web Console to do the following:

- Monitor the state of your organization's security system.
- Manage installed applications.
- View reports on the security system state.

Information about Kaspersky IoT Secure Gateway 1000 may not be displayed when viewing information about the device running Kaspersky IoT Secure Gateway 1000 in the Web Console on the **General** tab in the **General, Network, System, Protection, and Device status determined by application** sections.

Kaspersky IoT Secure Gateway 1000 is synchronized with Kaspersky Security Center every 30 seconds, which is known as the "heartbeat" interval. At this interval, the Kaspersky Security Center 14.2 Web Console receives information about events registered in Kaspersky IoT Secure Gateway 1000, and any settings that are defined in the Kaspersky IoT Secure Gateway 1000 interface or in the Web Console are synchronized.

About the Kaspersky IoT Secure Gateway 1000 administration web plug-in

The Kaspersky IoT Secure Gateway 1000 administration web plug-in (hereinafter also referred to as simply "the web plug-in") facilitates interaction between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console.

The web plug-in lets you centrally perform the following actions through the Kaspersky Security Center 14.2 Web Console:

- [Configure the settings of Kaspersky IoT Secure Gateway 1000.](#)
- [Receive events from Kaspersky IoT Secure Gateway 1000.](#)
- [Manage the firewall.](#)
- [Manage the Kaspersky IoT Secure Gateway Network Protector settings and IP address denylists and allowlists.](#)
- [Manage the security of Kaspersky IoT Secure Gateway 1000.](#)
- [Update](#) and [restart](#) Kaspersky IoT Secure Gateway 1000.
- [Manage applications and their configuration.](#)

Installing the Kaspersky IoT Secure Gateway 1000 administration web plug-in

The Kaspersky IoT Secure Gateway 1000 administration web plug-in is not installed in the Kaspersky Security Center 14.2 Web Console by default. The Kaspersky IoT Secure Gateway 1000 administration web plug-in is included in the [Kaspersky IoT Secure Gateway 1000 distribution kit](#). You need to install the web plug-in on the computer that has the Kaspersky Security Center 14.2 Web Console installed. The web plug-in functionality is available to all administrators that can access the Kaspersky Security Center 14.2 Web Console in a browser. The list of installed web plug-ins is displayed in the Kaspersky Security Center 14.2 Web Console interface (**Console settings** → **Web plug-ins**).

Port 13294 must be accessible on the Administration Server where Kaspersky Security Center is installed. Port 13294 is required for connecting UEFI protection devices. For more details about managing UEFI protection devices, please refer to the *UEFI protection devices* section in the Kaspersky Security Center 14.2 Online Help Guide. For more details about the ports used for connecting to Kaspersky Security Center, please refer to the section titled *Ports used by Kaspersky Security Center* in the Kaspersky Security Center 14.2 Online Help Guide.

Kaspersky Security Center 14.2 and Kaspersky Security Center 14.2 Web Console are not included in the [Kaspersky IoT Secure Gateway 1000 distribution kit](#). They must be installed separately.

To install the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 14.2 Web Console:

1. In the Kaspersky Security Center 14.2 Web Console menu, select **Console settings** → **Web plug-ins**.
A list of available administration plug-ins for the Kaspersky Security Center 14.2 Web Console will appear.
2. Click the **Add from file** button.
3. In the opened pane on the right, add the following files:
 - ZIP archive containing the web plug-in distribution package received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download ZIP file** button.
 - Signature file received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download signature** button.
4. Click the **Add** button.
5. When installation of the web plug-in is complete, click **OK**.

The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be loaded into the default configuration and will appear in the list of Kaspersky Security Center 14.2 Web Console administration plug-ins.

Updating the Kaspersky IoT Secure Gateway 1000 administration web plug-in

You can update the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 14.2 Web Console.

To update the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 14.2 Web Console:

1. In the Kaspersky Security Center 14.2 Web Console menu, select **Console settings** → **Web plug-ins**.

A list of available administration plug-ins for the Kaspersky Security Center 14.2 Web Console will appear.

2. In the list of administration plug-ins, select the check box next to the Kaspersky IoT Secure Gateway 1000 administration web plug-in.

3. Click the **Update from file** button.

4. In the opened pane on the right, add the following files:

- ZIP archive containing the web plug-in distribution package received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download ZIP file** button.
- Signature file received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download signature** button.

5. Click **Update**.

6. When the update is complete, click **OK**.

The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be updated, and its version information and update time will be displayed in the table of administration web plug-ins in the Kaspersky Security Center 14.2 Web Console.

Removing the Kaspersky IoT Secure Gateway 1000 administration web plug-in

The Kaspersky IoT Secure Gateway 1000 administration web plug-in can be removed in the Kaspersky Security Center 14.2 Web Console. After the web plug-in is removed, you will not be able to manage Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console.

To remove the Kaspersky IoT Secure Gateway 1000 administration web plug-in from the Kaspersky Security Center 14.2 Web Console:

1. In the web interface menu of the Kaspersky Security Center 14.2 Web Console, select **Console settings** → **Web plug-ins**.

A list of available administration plug-ins for the Kaspersky Security Center 14.2 Web Console will appear.

2. In the list of administration plug-ins, select the check box next to the Kaspersky IoT Secure Gateway 1000 administration web plug-in.

3. Click the **Delete** button.

4. In the plug-in removal confirmation window that opens, do one of the following:

- If you need to save a backup copy of the plug-in, click **OK**.

A backup copy of the plug-in will be created. The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be removed from the Kaspersky Security Center 14.2 Web Console.

- If you do not need to save a backup copy of the plug-in, click the **Skip data backup** button.

The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be removed from the Kaspersky Security Center 14.2 Web Console.

5. In the opened window containing information about plug-in removal, click **OK**.

Logging in and logging out of the Kaspersky Security Center 14.2 Web Console

To log in to the Kaspersky Security Center 14.2 Web Console, you need to ask the administrator for the web address of the Kaspersky Security Center Administration Server and the port number that was specified during installation (port 8080 is used by default). You must also enable JavaScript in your browser.

To log in to the Kaspersky Security Center 14.2 Web Console:

1. In your browser, open `https://<address>:<port>`.

For the requirements of the browser used to work with the Kaspersky Security Center 14.2 Web Console, please refer to the *Hardware and software requirements* section of the *Kaspersky Security Center 14.2 Online Help Guide*.

The login page opens.

2. Log in using the user name and password of a local administrator.

If the Kaspersky Security Center Administration Server does not respond or you entered incorrect account credentials, an error message will be displayed.

After logging in, the Dashboard appears displaying the last language and theme that were used.

If you are logging in to the Kaspersky Security Center 14.2 Web Console for the first time, a tutorial is displayed in the lower part of the screen. You can follow the instructions of the tutorial, or close it.

You are now logged in to Kaspersky Security Center 14.2 Web Console and can work with the Kaspersky Security Center 14.2 Web Console. For additional information about how the Kaspersky Security Center 14.2 Web Console works, please refer to the Online Help Guide for Kaspersky Security Center 14.2.

To log out of the Kaspersky Security Center 14.2 Web Console:

1. In the menu of the Kaspersky Security Center 14.2 Web Console, click the user name.

2. In the opened menu, select **Log out**.

The Kaspersky Security Center 14.2 Web Console closes and the login page is displayed.

Adding a Kaspersky IoT Secure Gateway 1000 device to the group of managed devices of the Kaspersky Security Center 14.2 Web Console

To use the Kaspersky Security Center 14.2 Web Console to manage a device with Kaspersky IoT Secure Gateway 1000 installed, move this device to the group of managed devices.

To add a device to the group of managed devices in the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Kaspersky Security Center 14.2 Web Console, select **Device discovery and deployment** → **Unassigned devices**.

The list of all detected unassigned devices will be displayed.

2. Select the check box next to the name of the device that you want to add to the group of managed devices.
3. Click the **Move to group** button.
The **Move to group** pane opens on the right.
4. Select the check box next to the **Managed devices** administration group.
5. Click the **Move** button.

The device will be moved to the managed devices group.

Configuring Kaspersky IoT Secure Gateway 1000 settings through the Web Console

This section contains information about configuring Kaspersky IoT Secure Gateway 1000 settings through the Web Console.

Configuring MQTT broker settings through the Web Console



Configuration of the MQTT broker settings is available only to the [network router device type](#).

This section contains information about configuring MQTT broker settings through the Web Console. In the Kaspersky Security Center 14.2 Web Console, you can create new [MQTT broker profiles](#), edit existing profiles, and switch between profiles.

To view the MQTT broker profiles table through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT Broker** section.

The table of MQTT broker profiles is displayed. The table shows the following information for each MQTT broker profile:

- **Access** – profile editing access. This lock  icon, indicating that the profile is read-only, is only displayed for predefined profiles provided with the device.
- **Status** – the  icon indicates that the MQTT broker profile is currently in use.

- **Name** – name of the profile.
- **Modified** – date and time of the most recent change in the profile.

Creating an MQTT broker profile through the Web Console

You can create new MQTT broker profiles through the Kaspersky Security Center 14.2 Web Console. Different MQTT broker profiles let you work with different servers and digital platforms that receive events from Kaspersky IoT Secure Gateway 1000 over the MQTT protocol.

To create a new MQTT broker profile through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT Broker** section.
The table of MQTT broker profiles is displayed.
7. Click the **Add** button in the upper part of the MQTT broker profiles table.
The **Edit profile** window opens.
8. In the **Status** drop-down list, select one of the following values:
 - **Active**, if you want to make a new profile active. In this case, profile settings are uploaded to the MQTT broker and access to certificates from the profile is activated for the MQTT broker.
 - **Inactive**.

Only one profile can be active. You can only set an MQTT broker profile as active if it has a configuration file added.

9. In the **Name** field, enter the profile name using letters of the English alphabet.
10. Add a configuration file or certificate to the new profile by clicking the **Add** button in the upper part of the **List of files** table.
11. In the file upload pane that opens on the right, do the following:
 - a. In the **Type** drop-down list, select the type of file that you want to add:
 - **Configuration file**. This contains the main settings for MQTT broker operation. The configuration file must be added to the MQTT broker profile so that this profile can be set as active. Files in CONF format

can be selected.

- **Certificate.** Files in CRT, CER, DER, and PEM format can be selected.

An MQTT broker profile requires multiple security certificates, such as a certificate issued by a Certificate Authority, a server client certificate, and a private key file. Depending on the requirements of the MQTT server, the server client certificate and private key file must be signed with a valid certificate issued by a certification authority. If your profile prescribes the use of SSL/TLS, repeat this step as many times as required to upload all required certificates to the system. A secure connection is not guaranteed in the absence of security certificates.

We do not recommend uploading more than three security certificate files per MQTT profile. If more than three files are uploaded, only the last uploaded certificate files will be used.

- b. Click the **Upload file** button and select a file in the opened file upload window. The file size must not exceed 131 KB.

The file will be uploaded to the system and will appear in the MQTT broker profile.

- c. Click **OK** in the lower part of the pane.

The file upload pane closes.

12. Click **OK** in the lower part of the **Edit profile** window.

The **Edit profile** window closes.

13. Click **Save** in the lower part of the window to save the new MQTT broker profile.

Editing an MQTT broker profile through the Web Console

To edit an MQTT broker profile through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT Broker** section.
The table of MQTT broker profiles is displayed.
7. In the MQTT broker profiles table, select the profile that you want to edit and click the **Edit** button in the upper part of the table.
The **Edit profile** window opens.

8. If you need to change the profile name, enter the profile name using letters of the English alphabet in the **Name** field.

For a profile provided together with the device (predefined profile), the **Name** field cannot be edited.

9. If you want to add a configuration file or certificate to the profile, click the **Add** button in the upper part of the **List of files** table.

The file upload pane opens on the right.

a. In the **Type** drop-down list, select the type of file that you want to add:

- **Configuration file.** This contains the main settings for MQTT broker operation. The configuration file must be added to the MQTT broker profile so that this profile can be activated. Files in CONF format can be selected.
- **Certificate.** Files in CRT, CER, DER, and PEM format can be selected.

An MQTT broker profile requires multiple security certificates, such as a certificate issued by a Certificate Authority, a server client certificate, and a private key file. Depending on the requirements of the MQTT server, the server client certificate and private key file must be signed with a valid certificate issued by a certification authority. If your profile prescribes the use of SSL/TLS, repeat this step as many times as required to upload all required certificates to the system. A secure connection is not guaranteed in the absence of security certificates.

We do not recommend uploading more than three security certificate files per MQTT profile. If more than three files are uploaded, only the last uploaded certificate files will be used.

b. Click the **Upload file** button and select a file in the opened file upload window. The file size must not exceed 131 KB.

The file will be uploaded to the system and will appear in the profile.

c. Click **OK** in the lower part of the pane.

The file upload pane closes. The file will be added to the MQTT broker profile and will appear in the **List of files** table.

10. If you want to delete a previously added configuration file or certificate in the MQTT broker profile, select the file that you want to delete and click the **Delete** button in the upper part of the **List of files** table.

The file will be deleted from the MQTT broker profile.

Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined MQTT broker profile files. If you need to delete active profile files, you have to [switch to a different MQTT broker profile](#) first.

11. Click **OK** in the lower part of the **Edit profile** window.

The **Edit profile** window closes.

12. Click **Save** in the lower part of the window to save the changes.


Switching to another MQTT broker profile through the Web Console

To edit an MQTT broker profile through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT Broker** section.
The table of MQTT broker profiles is displayed.
7. In the MQTT broker profiles table, select the profile that you want to edit and click the **Edit** button in the upper part of the table.
The **Edit profile** window opens.
8. In the **Status** drop-down list, select **Active** if you want to make this profile active. In this case, profile settings are uploaded to the MQTT broker and access to certificates from the profile is activated for the broker.

Only one profile can be active.

9. Click **OK** in the lower part of the **Edit profile** window.
The **Edit profile** window closes.
10. Click **Save** in the lower part of the window to save the changes.

In the profile table, in the **Status** column, the  icon appears next to the selected profile. The profile is now active and is used by Kaspersky IoT Secure Gateway 1000 when receiving data over the MQTT protocol.

Deleting an MQTT broker profile through the Web Console

Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined MQTT broker profile. If you need to delete the profile that is currently the active profile, you must first [select a different MQTT broker profile as active](#).

To delete an MQTT broker profile through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.
6. Select the **MQTT Broker** section.
7. In the table of MQTT broker profiles, select the profile that you want to delete and click the **Delete** button in the upper part of the table.
8. Click **Save** in the lower part of the window to save the changes.

The selected MQTT broker profile will be deleted.

Configuring internal and external network settings through the Web Console

Kaspersky IoT Secure Gateway 1000 is delivered with a statically configured IP address. To enable the system to operate as an Internet of Things (IoT) Secure Gateway, you must configure the settings of the external and internal networks. You can also [configure the network settings by using the web interface](#) of Kaspersky IoT Secure Gateway 1000.

To configure network settings through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.
6. Select **Network** → **LAN** and configure the following settings:
 - a. In the **IP address** field, enter the IP address of the Kaspersky IoT Secure Gateway 1000 device in the internal network.
 - b. In the **Subnet mask** field, enter the subnet mask.
 - c. If you need Kaspersky IoT Secure Gateway 1000 to act as a DHCP server, toggle **Use DHCP server** on and specify the following settings:
 - In the **Start of IP address range** field, enter the starting IP address of the range.
 - In the **End of IP address range** field, enter the ending IP address of the range.
 - In the **Primary DNS server address** field, enter the IP address of the primary DNS server.
 - In the **Secondary DNS server address** field, enter the IP address of the secondary DNS server.

The **MAC address** field displays the MAC address of the device in the internal network.

7. Click **Save** in the lower part of the window to save the changes.

8. Select **Network** → **WAN** and under **External network settings**, configure the following:

- If you want to configure network settings automatically using the DHCP protocol, set the **Automatic (via DHCP)** toggle button to the enabled position.

If the DHCP server issued null DNS server addresses to Kaspersky IoT Secure Gateway 1000 when enabling automatic configuration of external network settings, the IP address 208.67.222.222 (OpenDNS server) will be used by default to convert a domain name to an IP address.

- If you want to manually configure the external network settings, toggle **Automatic (via DHCP)** off and do the following:
 - In the **IP address** field, enter the IP address that you want to assign to the system in the external network.
 - In the **Subnet mask** field, enter the subnet mask.
 - In the **Default gateway** field, enter the IP address of the network gateway.
 - In the **Primary DNS server address** field, enter the IP address of the primary DNS server.
 - In the **Secondary DNS server address** field, enter the IP address of the secondary DNS server.

The **MAC address** field displays the MAC address of the device in the external network.

- If you want to [enable network address translation for the external network](#), toggle the **Enable masquerading** button on.

9. Click **Save** in the lower part of the window to save the changes.

Configuring masquerading through the Web Console

You can configure network address translation for the primary communication channel by using the masquerading functionality in Web Console.

Masquerading is a type of network address translation, in which the sender's address in the internal network is dynamically replaced with an address in the external network, depending on the address assigned to the interface. You can use the masquerading functionality if you need to spoof the parameters in the headers of IP packets for devices on the internal network or to hide an infrastructure behind one address. This will allow devices that reside in the internal network and do not have real IP addresses to send and receive IP packets from an external network.

To enable masquerading for the main communication channel in Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **WAN**.

7. In the **Broadcast settings** subsection, toggle on **Enable masquerading**.

Masquerading will be applied only to the communication channel designated as main: [external network](#) or [modem](#).

Adding a device name through the Web Console

To assign a device name through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings** → **Device name**.

7. Enter the name in the **Device name** field.

The device name can contain only numbers and letters of the English alphabet. The maximum name length is 32 characters.

8. Click **Save** in the lower part of the window to save the changes.

Managing certificates through the Web Console

You can view the previously uploaded [root certificate and Kaspersky Security Center Administration Server certificate](#), and update these through the Web Console.

Loading widely known Certification Authority certificates is not recommended, as all servers that use certificates signed by these Certification Authority certificates will be trusted. This situation can lead to Kaspersky IoT Secure Gateway 1000 being compromised.

The correct valid certificate file must be uploaded. Uploading the wrong certificate file may result in the device becoming inoperable.

To upload or update the Kaspersky IoT Secure Gateway 1000 root certificate through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Certificates**.
A window will be displayed containing information about the root certificate and the Kaspersky Security Center Administration Server certificate if loaded.
7. If you need to add a new root certificate, click **Upload** in the **Root certificate** section and select the certificate file in the window that opens. Only files in CRT, PEM, DER, or CER format can be added as a certificate.
The root certificate will be uploaded to the system.
8. If you have an uploaded root certificate and need to update it, in the **Root certificate** section, click **Update** and select the certificate file in the window that opens. Only files in CRT, PEM, DER, or CER format can be added as a certificate.
The new root certificate will upload to the system and the previously uploaded certificate will be deleted.

Kaspersky IoT Secure Gateway 1000 does not let you delete a root certificate without replacing the certificate with a new one.

9. Click **Save** in the lower part of the window to save the changes.

To upload or renew the Kaspersky Security Center Administration Server certificate through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Certificates**.
A window will be displayed containing information about the administrator certificate and the Kaspersky Security Center Administration Server certificate if loaded.

If a new certificate was issued for the Kaspersky Security Center Administration Server, the connection that was previously established between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center will be terminated. To resume the connection, you need to [add the newly issued certificate as a Kaspersky Security Center Administration Server certificate](#) in the Kaspersky IoT Secure Gateway 1000 web interface.

7. If you need to upload a new administrator certificate, click **Upload** in the **KSC server certificate** subsection and select the certificate file in the window that opens. Only files in CRT, PEM, DER, or CER format can be added as a certificate.

The Kaspersky Security Center Administration Server certificate will be uploaded to the system.

8. If you have an uploaded administrator certificate and you need to update it, in the **KSC server certificate** subsection, click **Update** and select the certificate file in the window that opens. Only files in CRT, PEM, DER, or CER format can be added as a certificate.

The new Kaspersky Security Center Administration Server certificate will be uploaded to the system and the previously uploaded certificate will be deleted.

Kaspersky IoT Secure Gateway 1000 prevents deleting a Kaspersky Security Center Administration Server certificate without replacing the certificate with a new one.

9. Click **Save** in the lower part of the window to save the changes.

Configuring routing via the Web Console

You can configure routing for more flexible management of network packets that pass through a device with Kaspersky IoT Secure Gateway 1000.

Data transfer using static routes for the internal network is possible only for the [network router device type](#).

To view the routing table of Kaspersky IoT Secure Gateway 1000:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Routing**.
7. Kaspersky IoT Secure Gateway 1000 will display the routing table containing the following information:

- **Type** – type of route:

- **Static** – route for which the settings for routing network packets were manually defined.
- **Dynamic** – route for which the settings for routing network packets are automatically determined by using a DHCP server, for example.
- **IP address** – IP address of the destination node or network.
- **Mask** – destination network mask.
- **Gateway** – IP address of the gateway in the network to which you need to transmit the traffic on the way to the specified IP address of the destination node or network.
- **Status** – route state:
 - **Active** – the route was applied and is used for data transmission.
 - **Error** – the route was not applied and cannot be used for data transmission because an error was made when creating the route. The error description is displayed on the right of the state. The **Error** state is displayed if the IP address of the gateway in the network is unreachable or if an invalid IP address or network mask was indicated as the destination node or network.
 - **Pending** – intermediate state. After synchronization with Kaspersky IoT Secure Gateway 1000 is complete, the current state is changed to **Active** or **Error**.

You can [create](#), [edit](#) and [delete](#) routes of Kaspersky IoT Secure Gateway 1000 via the Web Console. You can also [configure routing](#) in the Kaspersky IoT Secure Gateway 1000 interface.

Creating a static route via the Web Console

You can create new static routes for Kaspersky IoT Secure Gateway 1000 via the Web Console.

Kaspersky IoT Secure Gateway 1000 does not let you create duplicate default routes (second route for the IP address of the destination network 0.0.0.0/0) and routes in which an IP address in the network 127.0.0.0/8 is indicated as the IP address of the destination node.

When creating overlapping routes, you are advised to keep in mind that the route with the longer mask describing a smaller number of destination nodes will be selected to send a network packet to the IP address of the destination node or network.

To create a new static route for Kaspersky IoT Secure Gateway 1000 via the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.

6. Select **Network** → **Routing**.

This opens a window containing the routing table of Kaspersky IoT Secure Gateway 1000.

7. Click the **Add** button in the upper part of the page.

8. In the **Add route** pane that opens on the right, enter the following data:

- In the **IP address** field, enter the IP address of the destination node or network.
- In the **Mask** field, enter the destination network mask.
- In the **Gateway** field, enter the IP address of the gateway. The gateway IP address must be reachable.

The gateway IP address is reachable if this IP address resides within a connected network and is one of the nodes of a network configured on the internal or external interface.

9. Click **OK** in the lower part of the pane to save your changes.

The new static route is created and displayed in the routing table.

Editing a static route via the Web Console

To edit a static route of Kaspersky IoT Secure Gateway 1000 via the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **Routing**.

This opens a window containing the routing table of Kaspersky IoT Secure Gateway 1000.

7. In the table, select the check box next to the route that you need to edit and click the **Edit** button in the upper part of the table.

8. In the **Edit route** pane that opens on the right, make the necessary changes and click **OK** to save your changes.

The static route is changed, and the new data on this route is displayed in the routing table.

Deleting a static route via the Web Console

To remove a static route of Kaspersky IoT Secure Gateway 1000 via the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Routing**.
This opens a window containing the routing table of Kaspersky IoT Secure Gateway 1000.
7. In the table, select the check box next to the route that you need to remove, click **Delete** in the upper part of the table, and confirm the deletion.

The static route will be deleted from the routing table.

Configuring Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Web Console

If the device is not connected to a modem, you cannot use a cellular connection in Kaspersky IoT Secure Gateway 1000 or configure the connection settings through the Web Console.

You can view and configure the Kaspersky IoT Secure Gateway 1000 cellular connection settings in the Web Console under **Network** → **Modem**. This section contains the following information about the cellular connection of Kaspersky IoT Secure Gateway 1000:

- The **Modem settings** block provides information about the modem operating status and current signal quality.
- The **Modem DNS server addresses** block provides information about the IP addresses of the primary and secondary DNS servers of the modem.
- The **Modem profiles** table displays information about the [available modem profiles](#).
- The **Broadcast settings** section, where you can configure the use of masquerading for the cellular connection.
When masquerading is enabled, the sender's address on the internal network is dynamically replaced with an address on the external network, depending on the address assigned to the interface.

Kaspersky IoT Secure Gateway 1000 provides for two types of modem profiles:

- *Predefined profile* – a profile provided together with the device. Predefined profiles are read-only.
- *Custom profile* – a profile that is created during configuration of the cellular connection. Custom profiles can be edited and deleted.

Different modem profiles enable you to work with different cellular communication providers. To use a cellular connection, one of the modem profiles must be active. The predefined modem profile is active by default.

If there is no cellular connection, you must verify that the following conditions are met:

- The SIM card used in the modem is valid and has an active plan that supports an Internet connection through the modem.
- The selected modem profile matches the utilized SIM card.
- The modem is available for use (the **Enabled** modem status is displayed).

If the modem is not available for use (the **Not available** modem status is displayed), [restart Kaspersky IoT Secure Gateway 1000](#) and check the modem availability again. Devices that access the Internet through Kaspersky IoT Secure Gateway 1000 must obtain the internal network settings through the DHCP server of Kaspersky IoT Secure Gateway 1000. The relevant addresses of DNS servers from cellular network providers will be received together with these settings.

Enabling and disabling the Kaspersky IoT Secure Gateway 1000 cellular connection through the Web Console

Kaspersky IoT Secure Gateway 1000 lets you process outgoing and incoming network traffic using a cellular connection (through a cellular communications provider). You can enable or disable use of a Kaspersky IoT Secure Gateway 1000 cellular connection through the Kaspersky Security Center 14.2 Web Console. Use of a cellular connection is disabled by default.

To enable or disable the use of a Kaspersky IoT Secure Gateway 1000 cellular connection through the Web Console:


1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.
7. In the **Modem settings** block, move the toggle button to **Use modem as main communication channel** to enable use of the cellular connection, or move it to **Do not use modem as main communication channel** to disable use of the cellular connection.

The Kaspersky IoT Secure Gateway 1000 cellular connection will be enabled or disabled according to your selection. You can [enable network address translation for the modem](#) if necessary.

Creating a modem profile for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console

You can create new modem profiles for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console. Different modem profiles enable you to work with different cellular communication providers.

To create a new modem profile for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.
7. In the **Modem profiles** table, click the **Add** button.
The pane for adding a modem profile opens on the right.
8. In the **Status** drop-down list, select the profile status. The following values are available:
 - **Active**. The selected modem profile will be used as the main modem profile for the cellular connection of Kaspersky IoT Secure Gateway 1000. The  icon appears next to the active profile in the **Status** column of the **Profiles** table.
 - **Inactive**.
9. In the **Profile name** field, enter the profile name.
10. In the **Configuration file** field, enter the modem profile configuration settings.
11. Click **OK** in the lower part of the pane.
The pane for adding a modem profile will close. The new profile will be displayed in the **Modem profiles** table.
12. Click **Save** in the lower part of the modem settings window to save the changes.

Editing the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console

You can change the settings of the Kaspersky IoT Secure Gateway 1000 modem profile through the Kaspersky Security Center 14.2 Web Console.

To change the settings of the Kaspersky IoT Secure Gateway 1000 modem profile through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.


5. Select the **Application settings** tab.

6. Select **Network** → **Modem**.

7. In the **Modem profiles** table, select the check box next to the modem profile that you need to edit and click the **Edit** button in the upper part of the table.

8. In the modem profile editing pane that opens on the right:

a. Select one of the following values from the **Status** drop-down list if you need to change the status of a profile:

- **Active.** After saving the changes, the selected modem profile will be used as the main modem profile for the cellular connection of Kaspersky IoT Secure Gateway 1000. The  icon appears next to the active profile in the **Status** column of the **Profiles** table.
- **Inactive.**

When the modem profile status is changed to **Active**, you must [restart](#) Kaspersky IoT Secure Gateway 1000 for this change to take effect.

b. If necessary, enter a new profile name in the **Profile name** field.

c. You can edit the current settings or enter new settings for the modem profile in the **Configuration file** field.

d. Click **OK** in the lower part of the pane.

The pane for editing the modem profile will close. The modified profile will be displayed in the **Modem profiles** table.

9. Click **Save** in the lower part of the modem settings window to save the changes.

Deleting the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console

You can delete a modem profile through the Kaspersky Security Center 14.2 Web Console.

Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined modem profile. If you need to delete the profile that is currently the active profile, you must first [select a different modem profile as active](#).

To delete a Kaspersky IoT Secure Gateway 1000 profile through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.
7. In the **Modem profiles** table, select the check box next to the modem profile that you need to delete and click the **Delete** button.
The selected modem profile will be deleted from the **Modem profiles** table.
8. Click **Save** in the lower part of the modem settings window to save the changes.
The selected modem profile will be deleted.

Configuring web server using the Web Console

Operation of the Kaspersky IoT Secure Gateway 1000 web interface is supported by a CivetWeb web server. Web server settings are stored in a configuration file, connection security is ensured by the web server certificate. Kaspersky IoT Secure Gateway 1000 is delivered with a predefined web server certificate signed by Kaspersky.

You can upload a new web server certificate and key using the Web Console.

If you did not [replace](#) the default web server certificate when connecting to the web interface of Kaspersky IoT Secure Gateway 1000 for the first time, you must replace the default web server certificate with the certificate used in your organization after your first connection to the Web Console.

To upload a new web server certificate:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Web server**.
7. To upload a certificate, in the **Web server certificate** section, do one of the following:
 - If you have not added a certificate, click the **Upload certificate** button, and in the upload window that opens select the certificate file in the CRT, CER, DER, or PEM format.
 - If you have already added a certificate and want to replace it, click the **Replace** button, and in the upload window that opens select the certificate file in the CRT, CER, DER, or PEM format.

The correct valid certificate file must be uploaded. Uploading the wrong certificate file may result in the device becoming inoperable.

8. To upload a certificate key, in the **Certificate key** subsection, do one of the following:

- If you have not added a key, click the **Upload key** button and in the upload window that opens select the key file in the KEY format.
- If you have already added a key and want to replace it, click the **Replace** button, and in the upload window that opens select the key file in the KEY format.

9. Click **Save** in the lower part of the page to save the changes.

In the **Settings** → **Web server** section, the following information about the used certificate and web server key is displayed.

- In the **Web server certificate** section:
 - **File name** – certificate file name and its format.
 - **Subject name** – information about the application for which the certificate is issued.
 - **Issuer** – information about the organization that issued the certificate.
 - **Valid until** – certificate expiration date and time.
- The **Certificate key** section displays **File name**: certificate key file name and format.

Filtering application protocol traffic in Web Console

You can configure traffic filtering for application protocols from Web Console. Filtering allows blocking or unblocking FTP, HTTP, MQTT, Modbus, SMTP, IMAP, and POP3 traffic.

For the MQTT protocol only version 3.1.1 filtering is supported. For SMTP protocol only basic SMTP filtering is supported. Extended SMTP protocol filtering is not supported.

To configure application protocol traffic filtering:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.

6. Select **Network** → **Filtering**.

7. Configure traffic filtering for application protocols as follows:

- Select the check box next to the protocols for which you want to block traffic.
- Clear the check box next to the protocols for which you want to allow traffic.

By default, traffic is allowed for all application protocols.

8. Click **Save** in the lower part of the page to save the changes.

Kaspersky IoT Secure Gateway 1000 blocks all traffic for selected application protocols except for service traffic and allows traffic for the application protocols for which you cleared the check box.

When receiving a traffic packet that contains signs of a blocked application protocol, Kaspersky IoT Secure Gateway 1000 terminates the connection through which this traffic was exchanged. Several packets required to establish a connection may pass through Kaspersky IoT Secure Gateway 1000 after the traffic is detected, but then the connection will be terminated.

Configuring the network cluster

You can combine multiple Kaspersky IoT Secure Gateway 1000 devices into a fault-tolerant network cluster in the internal network. Joining devices to a network cluster allows you to assign one primary device that receives and transmits traffic and one or several backup devices. If the primary device fails, the traffic is transmitted through the backup device.

The network cluster settings must be configured on each Kaspersky IoT Secure Gateway 1000 device that you want to add to the network cluster.

For security purposes, we recommend setting up Port Security on the ports to which Kaspersky IoT Secure Gateway 1000 is connected as a network cluster and fixing the MAC addresses in the allowlist, as well as blocking the sending of IP packets with the destination address 224.0.0.18/32 from other ports. This ensures that only devices with fixed MAC addresses from certain ports can send VRRP packets.

Devices within a network cluster are independent. Data and configuration are not synchronized between devices.

To configure a network cluster settings in the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **Network cluster**.

7. Set the toggle to **Enable network cluster** and configure the following settings:

a. In the **Device priority** field, enter the priority for the current device within the network cluster.

You can specify a value between 0 and 254. The priority determines the role of the device in the cluster. The device with the lowest priority value is considered to be the main device, and the devices with higher priority values are considered to be backup devices. The lower the priority value of the backup device, the higher the device is in the queue for the case of the primary device failure.

There can be only one primary device in a network cluster.

b. In the **Cluster IP address** field, enter the local IP address of the LAN cluster.

The specified IP address is deployed on the device.

c. In the **Cluster IP address mask** field, enter the IP address subnet mask of the network cluster.

d. In the **Cluster Identifier** field, enter a unique ID for the network cluster.

The ID is required for the cluster nodes to uniquely recognize each other. However, the use of the ID does not guarantee protection against the actions of third parties. When setting up the network, you also need to secure the cluster network loop.

To avoid ID overlap, we recommend specifying a custom ID value.

For each device that you want to combine into a network cluster, specify the same values for the virtual IP address, IP address mask, and cluster ID.

8. If you want to reset the specified network cluster settings, click the **Cancel** button.

9. Click **Save** to save the changes.

The device is added to the network cluster by the specified IP address.

Configuring notifications through the Kaspersky Security Center 14.2 Web Console

This section contains information about configuring notifications through the Kaspersky Security Center 14.2 Web Console for registration of [events](#) in the system.

Configuring push notifications to a Syslog server through the Kaspersky Security Center 14.2 Web Console

Kaspersky IoT Secure Gateway 1000 includes a Syslog client that you can use to forward event notifications to a Syslog server. You can configure forwarding of notifications to a Syslog server through the Kaspersky Security Center 14.2 Web Console.

To configure delivery of notifications to a Syslog server:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Notifications** → **Syslog**.
7. Set the toggle button in the upper part of the window to **Use Syslog server to send events** and specify the following settings:
 - In the **IP address** field, specify the IP address of the Syslog server.
 - In the **Port** field, specify the port that will be used for the connection.
 - In the **Mode** drop-down list, select one of the following connection options:
 - **UDP**.
 - **TCP**.
 - **TLS**.
 - If the TLS protocol is selected for forwarding logs, upload a security certificate. To do so, click the **Upload certificate** button and select the relevant security certificate in the opened window.
8. Click **Save** in the lower part of the page to save the changes.

Kaspersky IoT Secure Gateway 1000 will forward event notifications to the Syslog server.

Configuring delivery of MQTT notifications through the Kaspersky Security Center 14.2 Web Console

Kaspersky IoT Secure Gateway 1000 can forward notifications about audit events over the MQTT protocol. You can configure delivery of MQTT notifications through the Kaspersky Security Center 14.2 Web Console.

To enable forwarding of MQTT notifications through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings** → **Notifications** → **MQTT Notifications**.

7. Slide the toggle switch to **Use MQTT to send events**.

8. In the **Server address** field, enter the IP address of the utilized MQTT server.

9. In the **Port** field, enter the port number used for the connection with the MQTT server.

You can use ports 1883 and 8883 to connect Kaspersky IoT Secure Gateway 1000 to an MQTT server residing in the internal network.

You can use port 8883 to connect Kaspersky IoT Secure Gateway 1000 to an MQTT server residing in an external network.

10. In the **MQTT topic name** field, specify the name of the MQTT-topic for sending notifications.

11. If you need to send notifications about audit events from a specific user, set the **Use authentication** toggle button to the enabled position and fill in the **User name** and **Password** fields. You can contact the administrator of the utilized MQTT server to find out the account credentials of the user that will serve as the source of the sent notifications.

Sending notifications from a specific user is disabled by default.

12. If you need to use a secure SSL connection, set the **Use secure SSL connection** toggle button to the enabled position and do the following:

a. Upload a certificate issued by a Certificate Authority. To do so, click the **Upload certificate** button and select a certificate file on the local device.

Information about the uploaded certificate from a Certificate Authority will be displayed on the page.

Loading widely known Certification Authority certificates is not recommended, as all servers that use certificates signed by these Certification Authority certificates will be trusted. This situation can lead to Kaspersky IoT Secure Gateway 1000 being compromised.

b. Upload the client certificate. To do so, click the **Upload client certificate** button and select a certificate file on the local device.

Information about the uploaded client certificate will be displayed on the page.

c. Upload a key for the client certificate. To do so, click the **Upload key** button and select a key file on the local device.

Use of a secure SSL connection is disabled by default.

13. Click **Save** in the lower part of the page to save the changes.

Kaspersky IoT Secure Gateway 1000 will forward notifications about audit events over the MQTT protocol.

Managing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 14.2 Web Console

This section contains instructions on monitoring audit events registered in Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console.

Viewing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 14.2 Web Console

You can view audit events registered by Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console. Audit events include [operating system audit events](#) and [firewall audit events](#).

To view events registered by Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Click the **Events** tab.

This opens a window displaying a table of audit events registered on the device. The following information is displayed for each table entry:

- **Time** – date and time when the event was registered.
- **Event** – event text and description.
- **Severity level** – event severity level:
 - 4 – critical;
 - 3 – functional failure;
 - 2 – warning;
 - 1 – informational message.

Configuring registration of Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 14.2 Web Console

You can enable registration of [Kaspersky IoT Secure Gateway 1000 audit events](#) in the Kaspersky Security Center 14.2 Web Console and configure notifications for audit event registration. For detailed information on configuring notifications for audit event registration in the Web Console, please refer to the *Configuring notification delivery* section in the Kaspersky Security Center 14.2 Online Help Guide. To configure audit event registration, first, create a policy for the device that will serve as the source of audit events. For detailed information on creating a policy, refer to the *Creating a policy* section in the Kaspersky Security Center 14.2 Online Help.

Kaspersky IoT Secure Gateway 1000 version 3.0 does not support management of device groups using Kaspersky Security Center policies. However, you can manage each device separately.

Each audit event in Kaspersky Security Center has a certain severity level. Depending on how the event appeared, it can be assigned one of the following severity levels:

- A *critical* event is an event that indicates the occurrence of a critical issue that may lead to data loss, an operational malfunction, or a critical error.
- A *functional failure* is an event that indicates a serious issue, error, or malfunction during the operation of the system or while performing a procedure.
- A *warning* is an event that requires attention because it emphasizes important situations in the operation of Kaspersky IoT Secure Gateway 1000 and may indicate a possible issue in the future. Most events are designated as warnings if the system can be restored without loss of data or functional capabilities after such events occur.
- An *informational message* is an event that signifies the successful completion of an operation, proper system functioning or completion of a procedure.

If registration of [Kaspersky IoT Secure Gateway 1000 audit events](#) is disabled in the Web Console, audit events are not received and are not displayed in the Web Console. After event registration is enabled in the Web Console, only new audit events will be received. All audit events that were registered in Kaspersky IoT Secure Gateway 1000 prior to enabling event registration in the Web Console will not be forwarded to the Web Console. Instead, you can [view](#) them only in the Kaspersky IoT Secure Gateway 1000 web interface.

To enable registration of Kaspersky IoT Secure Gateway 1000 audit events in the Kaspersky Security Center 14.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Click the **Configure events** tab.
6. In the menu in the left part of the screen, select the severity level for which you want to enable event registration:
 - **Critical**.
 - **Functional failure**.

- **Warning.**
- **Informational message.**

A table of audit events for the selected severity level will be displayed.

7. Click the **Add event** button.
8. Select the check boxes next to the types of events for which you want to enable event registration in the Web Console, and click **OK**.
9. To save the changes, click the **Save** button.

The selected types of Kaspersky IoT Secure Gateway 1000 audit events for the selected severity level will be registered and saved on the Kaspersky Security Center Administration Server. The default storage time for events is 30 days.

Configuring address translation rules through the Web Console

Masquerading rules are available only to the [network router device type](#).

Kaspersky IoT Secure Gateway 1000 implements port forwarding (destination NAT): a type of address translation that replaces the sender's address on the external network with an address on the internal network, providing access from the external network to the internal network via individual ports. Address translation rules describe the settings for converting network addresses of IP packets sent to an internal network from devices residing within the external network.

All address translation rules are displayed in the table under **Network** → **NAT**. The following settings are displayed for each rule:

- **Network interface** – interface to which the **External network** or **Modem** rule applies.
- **External port** – transport port of the external interface for which the rule is applied.
- **Protocol** – protocol for which the **TCP** or **UDP** rule is applied.
- **IP address** – IP address of the destination node.
- **Port** – port of the destination node.
- **Comment** – rule description consisting of no more than 255 characters.

You can [create](#), [edit](#) and [delete](#) address translation rules.

Creating an address translation rule through the Web Console

To create a new address translation rule through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **NAT**.

This opens a window containing the address translation rules table of Kaspersky IoT Secure Gateway 1000.

7. Click the **Add** button in the upper part of the page.

8. In the **Add rule** pane that opens on the right, enter the following data:

- In the **Network interface** drop-down list, select the interface for which the rule is applied: **External network** or **Modem**.
- In the **External port** field, enter the transport port number of the external interface for which the rule will be applied.
- In the **Protocol** drop-down list, select one of the protocols for which the rule is applied: **TCP** or **UDP**.
- In the **IP address** field, enter the IP address of the destination node.
- In the **Port** field, enter the port of the destination node.
- In the **Comment** field, enter a rule description consisting of no more than 255 characters.

9. Click **OK** in the lower part of the pane to save your changes.

The new rule will be created and displayed in the address translation rules table.

Editing an address translation rule through the Web Console

To edit an address translation rule through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **NAT**.

This opens a window containing the address translation rules table of Kaspersky IoT Secure Gateway 1000.

7. In the table, select the check box next to the rule that you want to edit and click the **Edit** button in the upper part of the table.

8. In the **Edit rule** pane that opens on the right, make the necessary changes and click **OK** to save your changes.

The rule will be changed, and the new data on this rule will be displayed in the address translation rules table.

Deleting an address translation rule through the Web Console

To delete an address translation rule through the Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **NAT**.
This opens a window containing the address translation rules table of Kaspersky IoT Secure Gateway 1000.
7. In the table, select the rule you want to delete, in the upper part of the table, click **Delete** and confirm deletion.

The address translation rule is deleted from the rules table.

Kaspersky IoT Secure Gateway Network Protector application management

Kaspersky IoT Secure Gateway Network Protector lets you block IP addresses whose internal and external traffic must be blocked, and unblock IP addresses whose traffic must be allowed.

Kaspersky IoT Secure Gateway Network Protector can block IP addresses according to industrial packet analysis rules that include command filtering rules and anomaly detection. You can [define filtering rules](#) in the application settings.

If a rule is triggered, Kaspersky IoT Secure Gateway Network Protector blocks suspicious network traffic and adds the source IP address to the denylist. You can manually [delete](#) an IP address from the denylist if you want to allow traffic from that IP address.

Kaspersky IoT Secure Gateway Network Protector can create up to 1000 rules in the list of blocked IP addresses.

Kaspersky IoT Secure Gateway Network Protector sends information about the blocked traffic and IP addresses to Kaspersky IoT Secure Gateway 1000. An appropriate event is added to the [event log](#) in Kaspersky Security Center and the [firewall audit log](#) in the Kaspersky IoT Secure Gateway 1000 web interface.

The IP address allowlist contains the internal network's and external network's IP addresses whose network traffic is not blocked by Kaspersky IoT Secure Gateway 1000. You can manually [add](#) IP addresses of the devices whose traffic should be allowed to the allowlist. Network traffic from IP addresses of the new devices that appear in the network is allowed by default; these IP addresses are not blocked by the system. If necessary, you can also [remove](#) IP addresses of devices from the allowlist.

Configuring industrial protocol traffic filtering in Web Console

You can use the Kaspersky IoT Secure Gateway Network Protector application to configure rules for blocking and filtering industrial protocol traffic. Industrial traffic filtering uses packet analysis rules and includes the following checks:

- filtering of commands in the MQTT and Modbus protocols;
- Scanning for MQTT and Modbus traffic anomalies.

For Kaspersky IoT Secure Gateway Network Protector to work, you need to configure it first. When started without a completed configuration, Kaspersky IoT Secure Gateway 1000 [enters emergency mode](#), as it cannot receive traffic filtering rules to ensure a secure state.

To configure traffic filtering rules for industrial protocols:

1. Use Kaspersky Update Utility to download files with lists of supported network packet analysis rules:
 - The `industrial_commands.rules` file contains a list of supported command filtering rules for industrial protocols.
 - The `industrial_anomalies.rules` file contains a list of supported traffic anomaly detection rules for industrial protocols.

The identifier (sid) 90000001 is used for internal purposes and cannot be assigned to any rule.

For detailed information on using the utility, refer to the Kaspersky Update Utility documentation.

2. If required, select from these files the rules that you want to apply to industrial protocol traffic filtering.
3. Encode the list of rules for filtering commands and the list of anomaly detection rules as two separate Base64 strings.
4. In the main window of the Web Console, select **Devices** → **Managed devices**.
5. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
6. In the device properties window that opens, select the **Applications** tab.
7. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
8. Select the **Application settings** tab.
9. Select **Settings of apps** → **Applications**.

The installed apps table will be displayed.

10. [Stop](#) Kaspersky IoT Secure Gateway Network Protector if running.

While Kaspersky IoT Secure Gateway Network Protector is stopped, transit traffic on the device will be blocked to ensure the security of connected devices.

11. Click the name of Kaspersky IoT Secure Gateway Network Protector.

The **Kaspersky IoT Secure Gateway Network Protector application management** panel opens on the right.

12. Provide rules for filtering industrial protocol traffic:

- In the **Rules for filtering commands in industrial protocols** field, provide industrial command filtering rules in Base64 encoding.
- In the **Rules for searching anomalies in industrial protocols** field, provide anomaly detection rules for industrial traffic in Base64 encoding.

You can provide rules in one of the fields or in both.

For Kaspersky IoT Secure Gateway Network Protector to work, define at least one configuration setting, or else Kaspersky IoT Secure Gateway 1000 [will enter emergency mode](#) after you start it, as it cannot receive traffic filtering rules to ensure a secure state.

13. Click **Save** in the lower part of the panel to save the changes.

14. [Start](#) Kaspersky IoT Secure Gateway Network Protector.

Industrial protocol traffic will be filtered using the specified rules. If the rule is triggered, traffic that matches the rule is blocked, and the IP address where the traffic originated is added to the IP address denylist. The information that the IP address was blocked is sent to the Kaspersky IoT Secure Gateway 1000 firewall. The traffic blocking event is recorded in the [audit log](#).

Adding an IP address to the IP address allowlist

The IP addresses of devices whose network traffic should be allowed can be added to the allowlist.

To add an IP address to the IP address allowlist:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Network Protector**.

7. Click the **Show list** button next to the **IP address allowlist** header.

The **IP address allowlist** window will be displayed.

8. If you want to filter the list of IP addresses, click the **Filter** button, and define and apply filtering criteria.

9. Click the **Add** button.

10. In the **IP address (source)** field that opens on the right, specify the IP address from which you want to allow traffic.

The IP address must meet the following requirements:

- Contains four numbers from 0 to 255 and the delimiter . separating these.
- Does not start with 0.
- Is not blank.
- Does not match 255.255.255.255.

11. Click **Save** in the lower part of the pane.

12. Click **Save** at the bottom of the **IP address allowlist** page.

The device IP address will be added to the IP address allowlist. After synchronization between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console, any changes to the IP address allowlist will be forwarded to Kaspersky IoT Secure Gateway 1000.

Modifying an IP address in the IP address allowlist

The IP addresses of devices whose network traffic should be allowed can be added to the allowlist.

To add an IP address to the IP address allowlist:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **Network Protector**.

7. Click the **Show list** button next to the **IP address allowlist** header.

The **IP address allowlist** window will be displayed.

8. If you want to filter the list of IP addresses, click the **Filter** button, and define and apply filtering criteria.

9. Select the IP address of the device that you want to change and click **Edit** at the top of the table.

10. In the **IP address (source)** field in the panel that opens on the right, edit the IP address from which you want to allow traffic.

The IP address must meet the following requirements:

- Contains four numbers from 0 to 255 and the delimiter . separating these.
- Does not start with 0.
- Is not blank.
- Does not match 255.255.255.255.

11. Click **Save** in the lower part of the pane.

12. Click **Save** at the bottom of the **IP address allowlist** page.

The device IP address in the IP addresses allowlist is updated. After synchronization between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console, any changes to the IP address allowlist will be forwarded to Kaspersky IoT Secure Gateway 1000.

Deleting an IP address from the IP address allowlist

You can delete an IP address from the device IP address allowlist.

To delete an IP address from the IP address allowlist:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Network Protector**.
7. Click the **Show list** button next to the **IP address allowlist** header.
The **IP address allowlist** window will be displayed.
8. If you want to filter the list of IP addresses, click the **Filter** button, and define and apply filtering criteria.
9. Select the device IP address that you need to remove from the IP address allowlist and click the **Delete** button in the upper part of the table.
10. Click **Save** in the lower part of the pane.
11. Click **Save** at the bottom of the **IP address allowlist** page.

The selected IP address will be removed from the IP address allowlist. After synchronization between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console, any changes to the IP address allowlist will be forwarded to Kaspersky IoT Secure Gateway 1000.

Deleting an IP address from the IP address denylist

You can delete an IP address from the list of IP addresses of devices whose traffic must be blocked. The IP address denylist is generated from the [industrial protocol filtering rules](#).

To delete an IP address from the IP address denylist:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Network Protector**.
7. Click the **Show list** button next to the **IP address denylist** header.
The **IP address denylist** window will be displayed.
8. If you want to filter the list of IP addresses, click the **Filter** button, and define and apply filtering criteria.
9. Select the device IP address that you need to remove from the IP address denylist and click **Delete** in the upper part of the table.
10. Click **Save** in the lower part of the pane.
11. Click **Save** at the bottom of the **IP address allowlist** page.

The selected IP address will be removed from the IP address denylist. After synchronization between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 14.2 Web Console, changes in the IP address denylist will be forwarded to Kaspersky IoT Secure Gateway 1000.

Managing the firewall

You can use the Kaspersky IoT Secure Gateway 1000 firewall to monitor and filter inbound traffic from the internal and external networks. [Network traffic processing](#) is determined by the [firewall rules](#). Traffic that is not explicitly allowed by firewall rules is blocked.

Kaspersky IoT Secure Gateway 1000 firewall monitors the status of active network connections and analyzes traffic taking into account the connection settings. This allows response packets to go through the firewall to the network connection source using the same firewall rules.

By default, when Kaspersky IoT Secure Gateway 1000 is started, all traffic (except service traffic) from the internal network to the external network is blocked. After restarting Kaspersky IoT Secure Gateway 1000, the last up-to-date configuration of the firewall rules is loaded.

About Firewall rules

The firewall rules are divided into *preset* and *custom*. Kaspersky IoT Secure Gateway 1000 supports rules for the TCP and UDP protocols (only IPv4). Stateful Packet Inspection is enabled for these protocols. In addition, the Kaspersky IoT Secure Gateway 1000 firewall checks network traffic against the lists of [blocked](#) and [allowed](#) IP addresses.

Preset firewall rules

Preset rules are supplied as part of Kaspersky IoT Secure Gateway 1000 and ensure full operation of the Kaspersky IoT Secure Gateway 1000 firewall. These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console. Preset rules allow the following Kaspersky IoT Secure Gateway 1000 connection types:

- Outgoing connections with the Kaspersky Security Center 14.2 Web Console over the TCP protocol;
- Incoming connections with the local web server over the HTTPS protocol;
- Outgoing connections with the Syslog server over the TCP and UDP protocols;
- Outgoing and incoming connections with MQTT data sources over the TCP protocol;
- Outgoing and incoming connections with external and internal DNS servers over the UDP protocol;
- Outgoing and incoming connections with devices combined into a [network cluster](#) (if activated and configured).

Custom firewall rules

You can manually [create](#) custom firewall rules, and [edit](#) or [delete](#) rules of this type. Changes to the configuration of custom rules are applied to the system after Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center are synchronized. Custom firewall rules are checked in the order defined in the Kaspersky Security Center 14.2 Web Console, from top to bottom. You can create up to 512 custom firewall rules. Events of creation, modification, and deletion of custom rules, as well as of reaching their limit, are recorded in the [event log](#).

Custom rules can also be received from third-party intrusion detection tools that Kaspersky IoT Secure Gateway 1000 integrates with via Kaspersky Security Center OpenAPI™.

Kaspersky IoT Secure Gateway 1000 cannot independently detect attacks that originate on an external network. This requires integration with third-party intrusion detection tools. Kaspersky IoT Secure Gateway 1000 and intrusion detection tools must be connected to the same instance of Kaspersky Security Center Administration Server.

When suspicious network activity or a possible intrusion from an external network is detected, the third-party intrusion detection system sends a rule to Kaspersky IoT Secure Gateway 1000 to block the source of the suspicious network activity. Kaspersky IoT Secure Gateway 1000 creates the rule in the firewall and blocks the source IP address according to that rule.

The created rule remains valid indefinitely. You can [delete the rule](#) manually if needed.

You can view the table of custom firewall rules in Kaspersky Security Center 14.2 Web Console in the **Network** → **Firewall** section. The following information is displayed for each rule:

- **Rule status** – active status of the custom rule: **Enabled** or **Disabled**.
- **Action** – action to be applied to the traffic passing through the firewall: **Allow** or **Block**.
- **Zone** – custom rule scope: **Internal network** or **External network**.
- **IP address (source)** – IP address of the network traffic source.
- **Port (source)** – port of the network traffic source.
- **IP address (target)** – IP address of the network traffic destination.
- **Port (target)** – port of the network traffic destination.
- **Protocol** – protocol used when scanning the network traffic: **TCP, UDP**.

The following limitations apply to the custom firewall rules of Kaspersky IoT Secure Gateway 1000:

- It is not allowed to specify the device domain name as the source or destination of the network traffic (including localhost, which is the standard domain name for private IP addresses).
- It is not allowed to use service ports reserved by the system as source or destination ports: 53, 67, 68, 443, 13294, 1883, 8883, 514.

Procedure for processing network traffic

Kaspersky IoT Secure Gateway 1000 processes traffic at the packet level according to [firewall rules](#) and the [lists of allowed and blocked IP addresses](#).

Kaspersky IoT Secure Gateway 1000 stops processing a network packet on the first match with a rule; all the following rules are ignored.

The traffic processing procedure differs for [unidirectional gateway and network router device types](#). The type of network device is defined when [installing Kaspersky IoT Secure Gateway 1000](#).

Traffic processing procedure for the unidirectional gateway device type

If Kaspersky IoT Secure Gateway 1000 functions as unidirectional gateway, traffic processing rules are applied differently depending on the type of network.

For external network traffic, the rules are applied in the following order:

1. Diagnostic firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing traffic when starting Kaspersky IoT Secure Gateway 1000 self-diagnostics.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

2. Outgoing traffic allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing traffic from a device on an internal network to a device on the external network.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

3. Preset firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They allow traffic over the ICPM protocol.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

4. VPN application allow rules.

These rules are delivered automatically after the VPN application is [installed](#). They are required for allowing traffic initiated by the VPN application.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

5. Preset firewall block rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for blocking all incoming traffic.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

For internal network traffic, the rules are applied in the following order:

1. Diagnostic firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing traffic when starting Kaspersky IoT Secure Gateway 1000 self-diagnostics.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

2. Outgoing traffic allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing traffic between devices on the internal network.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

3. Preset firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They allow traffic over the ICPM and CARP protocols, as well as Kaspersky IoT Secure Gateway 1000 web interface traffic and the Kaspersky Security Center 14.2 Web Console traffic.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

4. Deny rules for application protocol traffic filtering.

You can [select application protocols](#) whose traffic you want to block. Traffic processing rules will be generated according to your choices.

5. Emergency support mode deny rules.

This list of rules applies only if [emergency support mode](#) is active. In that event, all traffic is blocked. You cannot modify these rules.

6. IP address allowlist.

With Kaspersky IoT Secure Gateway Network Protector, you can [add to the allowlist](#), [edit](#) and [delete](#) the IP addresses of devices whose traffic must be allowed.

7. IP address denylist.

The list is generated automatically from information about suspicious industrial traffic filtered with Kaspersky IoT Secure Gateway Network Protector rules. You can [set up filtering rules](#) to block traffic that uses industrial protocols. You can also [delete IP addresses](#) previously added to the IP address denylist, if required.

8. Custom firewall deny rules.

You can [create](#), [edit](#), or [delete](#) these rules for the internal and external networks.

9. Custom firewall allow rules.

You can [create](#), [edit](#), or [delete](#) these rules for the internal and external networks.

10. Preset Syslog and DHCP allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

11. Rules to allow outgoing traffic over established connections.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing outgoing traffic in response to incoming requests from an external network.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

12. Preset firewall block rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

Traffic processing procedure for the network router device type

If Kaspersky IoT Secure Gateway 1000 is functioning as a network router, traffic processing rules are applied in the following order:

1. Diagnostic firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing traffic when starting Kaspersky IoT Secure Gateway 1000 self-diagnostics.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

2. Preset firewall allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They allow traffic over the ICPM and CARP protocols, as well as Kaspersky IoT Secure Gateway 1000 web interface traffic and the Kaspersky Security Center 14.2 Web Console traffic.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

3. Deny rules for application protocol traffic filtering.

You can [select application protocols](#) whose traffic you want to block. Traffic processing rules will be generated according to your choices.

4. Emergency support mode deny rules.

This list of rules applies only if [emergency support mode](#) is active. In that event, all traffic is blocked. You cannot modify these rules.

5. IP address allowlist.

With Kaspersky IoT Secure Gateway Network Protector, you can [add to the allowlist](#), [edit](#) and [delete](#) the IP addresses of devices whose traffic must be allowed.

6. IP address denylist.

The list is generated automatically from information about suspicious industrial traffic filtered with Kaspersky IoT Secure Gateway Network Protector rules. You can [set up filtering rules](#) to block traffic that uses industrial protocols. You can also [delete IP addresses](#) previously added to the IP address denylist, if required.

7. Address translation (NAT) allow rules.

You can [create](#), [edit](#), and [delete](#) these rules.

8. Custom firewall deny rules.

You can [create](#), [edit](#), or [delete](#) these rules for the internal and external networks.

9. Custom firewall allow rules.

You can [create](#), [edit](#), or [delete](#) these rules for the internal and external networks.

10. Preset Syslog, MQTT, DHCP, and DNS allow rules.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

11. Rules to allow outgoing traffic over established connections.

These rules are supplied as part of Kaspersky IoT Secure Gateway 1000. They are required for allowing outgoing traffic in response to incoming requests from an external network.

These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

12. Preset firewall block rules.

These rules block all incoming traffic. They are supplied as part of Kaspersky IoT Secure Gateway 1000. These rules cannot be modified, and they are not displayed in Kaspersky Security Center 14.2 Web Console.

Creating firewall rules

Custom firewall rules are checked in the order defined in the Kaspersky Security Center 14.2 Web Console, from top to bottom until the first match.

You can create no more than 512 custom firewall rules in Kaspersky Security Center 14.2 Web Console.

To create a new firewall rule:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Firewall**.

This opens a table containing the custom firewall rules.

7. Click the **Add** button in the upper part of the firewall rules table.

The pane for adding a firewall rule opens on the right.

8. In the **Rule status** drop-down list, select the status of the rule: **Enabled** or **Disabled**.

9. In the **Action** drop-down list, select the action to apply to the traffic passing through the firewall: **Allow** or **Block**.

10. In the **Zone** drop-down list, select the zone to which the rule should be applied: **LAN** or **WAN**.

11. In the **IP address (source)** field, specify the IP address of the traffic source.

12. In the **Port (source)** field, specify the port of the traffic source if this parameter is applicable to the protocol.

13. In the **IP address (target)** field, specify the IP address of the traffic destination.

14. In the **Port (target)** field, specify the port of the traffic destination if this setting is applicable to the protocol.

15. In the **Protocol** drop-down list, select the utilized protocol. The available options are **TCP (IPv4)**, **UDP (IPv4)**, and **Any**.

16. Click **OK** in the pane for adding a firewall rule.

The pane closes, and the new rule is displayed in the firewall rules table.

17. If you need to change the order (priority) of a rule in the rules table, select the check box next to the rule and use the **Up** or **Down** button to raise or lower the rule priority.

18. Click the **Save** button.

Editing firewall rules

To edit a firewall rule:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **Firewall**.

This opens a table containing the custom firewall rules.

7. Select the check box next to the rule that you want to edit.

8. Click the **Edit** button in the upper part of the table.

The pane for editing a firewall rule opens on the right.

9. If you need to change the status of the rule, select a rule status from the **Status** drop-down list: **Enabled** or **Disabled**.

10. To change how traffic is handled by the firewall, in the **Action** drop-down list, select one of the available actions to apply to traffic passing through the firewall: **Allow** or **Block**.

11. If you need to change the direction of traffic, in the **Zone** drop-down list, select the zone to which the rule should be applied: **LAN** or **WAN**.

12. If necessary, change the IP address of the traffic source in the **IP address (source)** field.

13. If necessary, change the port of the traffic source in the **Port (source)** field if this parameter is applicable to the protocol.

14. If necessary, change the IP address of the recipient in the **IP address (target)** field.

15. If necessary, change the port of the recipient in the **Port (target)** field.

16. If necessary, select a protocol from the **Protocol** drop-down list. The available options are **TCP (IPv4)**, **UDP (IPv4)**, and **Any**.

17. Click **OK** in the pane for editing a firewall rule.

The pane closes, and the changed rule is displayed in the firewall rules table.

18. If you need to change the order (priority) of a rule in the rules table, select the check box next to the rule and use the **Up** or **Down** button to raise or lower the rule priority.

Custom firewall rules are checked according to their order in the rules table, from top to bottom until the first match.

19. Click the **Save** button.

Deleting firewall rules

To delete a firewall rule:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Network** → **Firewall**.

7. In the table that appears, select the check box next to the rule that you want to delete and click **Delete** at the top of the table.

The rule is deleted from the firewall rules table.

8. Click the **Save** button.

Updating Kaspersky IoT Secure Gateway 1000 through the Web Console

You can run a full update of Kaspersky IoT Secure Gateway 1000. The **Audit** section provides information about successful downloads and verification of updates, and information about completed updates of Kaspersky IoT Secure Gateway 1000. After Kaspersky IoT Secure Gateway 1000 is updated, the device will be restarted.

The system can be updated only if Kaspersky IoT Secure Gateway 1000 is connected to Kaspersky Security Center. A full update of Kaspersky IoT Secure Gateway 1000 from Kaspersky update servers is available in version 3.0 only.

To run a full update of Kaspersky IoT Secure Gateway 1000, do as follows:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings** → **Updates**.

7. In the **Full system update** subsection, click **Run update**.

Kaspersky IoT Secure Gateway 1000 will be fully updated. The device will be restarted during the update process.

Restarting Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console

To restart Kaspersky IoT Secure Gateway 1000:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select the **Synchronization** section.

7. In the **Commands** section, click **Restart device**, then click **Save** at the bottom of the page to send a restart command to the device.

The device running Kaspersky IoT Secure Gateway 1000 will be restarted. The connection Kaspersky Security Center and Kaspersky IoT Secure Gateway 1000 will be unavailable while the device is restarting

Managing Kaspersky IoT Secure Gateway 1000 apps through the Web Console

This section contains information about managing Kaspersky IoT Secure Gateway 1000 apps through the Web Console.

Working with applications via the Web Console

All apps available for [installation in Kaspersky IoT Secure Gateway 1000](#) are displayed in the Web Console on the **Application settings** → **App Manager** → **All apps** tab. The following information is displayed for each app in the table:

- **Name** – app name. You can view detailed information on an app by clicking its name.
- **Title** – a brief description of the application.
- **Version** – the number of the last application version available for installation.
- **Size** – the size of the application installation package.
- **Category** – categories the app belongs to.
- **Publication date** – date when the app was published in the app store.
- **Status** – installation status and availability of application installation. If the security of an application is compromised, a **Compromised** status is displayed for that application. A compromised application cannot be installed.

All apps installed in Kaspersky IoT Secure Gateway 1000 are displayed in the Web Console on the **Application settings** → **App Manager** → **Installed Apps** tab. The following information is displayed for each installed app in the table:

- **Name** – app name. You can view detailed information on an app by clicking its name.
- **Version** – the installed version of the application.
- **Publication date** – date when the app was published in the app store.
- **Category** – categories the app belongs to.
- **Status** – application status (installed, or error if the application could not be installed or uninstalled).

Applications installed in Kaspersky IoT Secure Gateway 1000 can be managed on the **Application Settings** → **Settings of apps** → **Applications** tab. The following information is displayed for each app in the table:

- **Name** – app name. If an application can be [configured](#), you can do it by clicking on its name.
- **Version**: the installed app version.
- **Application type** – the type of the application based on its function in Kaspersky IoT Secure Gateway 1000.
- **Status**: the application status (running or stopped).

- **Start rule:** the method used to start the app on the device: autorun, manual or blocked.
You can configure a start rule only for configured applications that have the **Run** or **Stopped** status.
- **Manifest** – application configuration file. To view the contents of the manifest, click **View**.

Under **Application settings** → **Settings of apps** → **Applications**, you can [start](#), [stop](#), or [uninstall](#) an application from the device.

Downloading and installing applications through the Web Console

You can download and install no more than 20 apps in Kaspersky IoT Secure Gateway 1000.

To download and install an app in Kaspersky IoT Secure Gateway 1000, do as follows:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **App Manager** → **All apps**.
The apps table will be displayed. The **Available for installation** status is displayed for apps that you can install in Kaspersky IoT Secure Gateway 1000.
7. Select the check boxes next to the apps that you want to download and install in Kaspersky IoT Secure Gateway 1000, and click **Save** in the lower part of the page.

All available apps are guaranteed to work for the [unidirectional gateway network device type](#). Only the Kaspersky IoT Secure Gateway Network Protector and Kaspersky Debug Service applications are guaranteed to work for the [network router device type](#). You can install other applications, but they are not guaranteed to work on the device.

The selected apps will be downloaded and installed in Kaspersky IoT Secure Gateway 1000. After Kaspersky IoT Secure Gateway 1000 is synchronized with Kaspersky Security Center, the **Installed** status will be displayed for these apps in the apps table. Information about successful or unsuccessful downloads and installations is saved in the [event log](#).

Installed applications are not updated automatically. To update an application, first [uninstall the currently installed version of the application](#) and then install the new version. If you uninstall a delisted (not displayed on the **All Apps** tab) version of an application, you cannot reinstall that version later.

Configuring app settings through the Web Console

After [installing the application](#) in Kaspersky IoT Secure Gateway 1000, it is recommended to configure it. The configuration settings for each application may differ, as they are defined by the publisher.

You can contact the publisher with questions about application configuration settings.

You can [set up start rules](#) for configured applications only.

To define application configuration settings, do as follows:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Applications**.
The installed apps table will be displayed.
7. Click the name of the application you want to configure.
The application settings panel opens on the right.
8. Configure the application settings as required.
9. Click **Save** in the lower part of the panel to save the changes.
The application settings panel closes.
10. Click **Save** in the lower part of the installed applications page to save the changes.
The application configuration settings will be applied.

Starting and stopping applications via the Web Console

To start or stop an app on a device:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings of apps** → **Applications**.

The installed apps table will be displayed.

7. Select the check box next to the applications that you want to start or stop and click **Start / Stop** at the top of the table.

For applications with a user interface that have a status of **Not configured**, you have to first [set up the configuration](#) and then wait for the status to change to **Stopped**.

When Kaspersky Security Center is synchronized with the device, the previously started app is stopped in Kaspersky IoT Secure Gateway 1000, and the previously stopped app is started.

Managing application start rules through the Web Console

You can configure how the application is started in Kaspersky IoT Secure Gateway 1000 (automatically or manually), or prevent the application from starting.

To configure the application start rules:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings of apps** → **Applications**.

The installed apps table will be displayed.

7. In the row of the application for which you want to configure a start rule, in the **Start rule** column, select one of the following values from the drop-down list:

- **Autostart** – the application starts automatically when Kaspersky IoT Secure Gateway 1000 is turned on or restarted.

You can manually stop and start the application if necessary.

- **Manual start**: the application starts only manually by clicking the **Start/Stop** button.

By default, the manual start rule is applied to the installed applications.

- **Block start** – the application is not available to start. The **Start/Stop** button is not available.

If you have changed the launch rule for a running application, the modified launch rule will be applied only after the applications are stopped. You can [manually stop the application](#) to apply the selected launch rule.

For apps with a user interface that have the **Not configured** status, you need to [set up the configuration first](#), and then wait for the status to change to **Run** or **Stopped**.

After Kaspersky Security Center is synchronized with the device, the launch rule for the selected app will be applied in Kaspersky IoT Secure Gateway 1000.

Removing applications via the Web Console

To remove an app from Kaspersky IoT Secure Gateway 1000:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **App Manager** → **Installed apps**.
The installed apps table will be displayed.
7. In the **Uninstall** column, select the check box next to the applications you want to uninstall and click **Save** in the lower part of the page.

The selected apps will be removed from the installed apps table. The [routes](#) associated with these apps stop working (their status changes to **Error**). It is recommended to reconfigure the routes associated with the deleted apps. When Kaspersky Security Center is synchronized with the device, the selected apps, their metadata, and the app event logs are removed from Kaspersky IoT Secure Gateway 1000. Information about successful or unsuccessful removal of apps is saved in the [events log](#).

Managing app certificates

An *application certificate* is a specialized digital signature file that ensures the safe operation of an application in Kaspersky IoT Secure Gateway 1000 and provides an encrypted communication channel for data exchange between the installed application and the application server. You can use a Certification Authority certificate and/or a client certificate. A key must also be added to the client certificate.

For apps installed in Kaspersky IoT Secure Gateway 1000, you can [add](#), [update](#) and [delete](#) certificates and their keys.

You can also view the current certificates in the Web Console under **Application settings** → **Settings of apps** → **Certificates**. Depending on the certificate type, the following information is displayed for each certificate:

- The following information is displayed for the certification authority certificate:
 - **File name** – certification authority certificate file name and format.

- **Subject** – information about the application for which the certification authority certificate is issued.
- **Issuer** contains information about the Certificate Authority that issued the certificate.
- **Valid until** – certification authority certificate validity end date.
- The following information is displayed for the client certificate:
 - **File name** – client certificate file name and format.
 - **Subject name** – information about the application for which the client certificate is issued.
 - **Issuer** – information about the organization that issued the certificate.
 - **Valid until** – client certificate validity end date.
- For a client certificate key, the key **File name** and format are displayed.

Adding application certificates

For the applications installed in Kaspersky IoT Secure Gateway 1000, you can add a full set of certificates, including the certification authority certificate and the client certificate, or only one of these certificates. A key must also be added for the client certificate.

To add a new certification authority certificate for an application:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Certification Authority certificate** block, click the **Upload certificate** button and select the certificate file in the opened window. Only files in CRT, CER, DER or PEM format can be uploaded.
The certificate file will be uploaded, and information about this certificate will be displayed on the page.
8. Click the **Save** button in the lower part of the page.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the certification authority certificate is also added to Kaspersky IoT Secure Gateway 1000. The installed application for which the certification authority certificate is issued uses the downloaded certificate.

To add a new client certificate for an application and a key for the certificate:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Client certificate** block:
 - Click the **Upload certificate** button and select the certificate file in the opened window. Only files in CRT, CER, DER or PEM format can be uploaded.
 - Click the **Upload key** button and select the key file in the opened window. Only key files in KEY format can be uploaded.

Certificate files and their keys will be uploaded, and information about them will be displayed on the page.

8. Click the **Save** button in the lower part of the page.
It is not possible to save changes if you have uploaded only the client certificate or only the key. Both files (the certificate and the key) must be uploaded to continue.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the client certificate and the key are also added to Kaspersky IoT Secure Gateway 1000. The installed application for which the client certificate is issued uses the downloaded certificate and the key.

Updating application certificates

To update a certification authority certificate for an application:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Certification Authority certificate** section, click the **Replace** button and select the new certificate file in the opened window. Only files in CRT, CER, DER or PEM format can be uploaded.

The certificate file will be updated, and information about the new certificate will be displayed on the page.

8. Click the **Save** button in the lower part of the page.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the certification authority certificate is also updated in Kaspersky IoT Secure Gateway 1000. The application for which the certificate is issued uses the downloaded certificate.

To update a client certificate for an application and the key for the certificate:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Client certificate** block:
 - In the **Certificate** section, click the **Replace** button and select the new certificate file in the opened window. Only files in CRT, CER, DER or PEM format can be uploaded.
 - In the **Certificate key** section, click the **Replace** button and select the new certificate key file in the opened window. Only key files in KEY format can be uploaded.

The certificate files and their keys will be updated, and information about them will be displayed on the page.

8. Click the **Save** button in the lower part of the page.

It is not possible to save changes if you have uploaded only the client certificate or only the key. Both files (the certificate and the key) must be uploaded to continue.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the client certificate and the key are also updated in Kaspersky IoT Secure Gateway 1000. The application for which the certificate is issued uses the downloaded certificate and the key.

Deleting application certificates

To delete a certification authority certificate for an application:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Certification Authority certificate** block, click the **Delete** button and confirm deletion.
The certificate file will be deleted.
8. Click the **Save** button in the lower part of the page.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the certification authority certificate is also deleted from Kaspersky IoT Secure Gateway 1000.

To delete a client certificate for an application and the key for the certificate:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Certificates**.
7. In the **Client certificate** block:
 - In the **Certificate** block, click the **Delete** button and confirm deletion.
 - In the **Certificate key** section, click the **Delete** button and confirm deletion.

The certificate files and their keys will be deleted.

8. Click the **Save** button in the lower part of the page.

After synchronization between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center, the client certificate and the key are also deleted from Kaspersky IoT Secure Gateway 1000.

Routing apps

You can configure routing of data between apps installed in Kaspersky IoT Secure Gateway 1000. Routes for the apps are displayed in the Web Console on the **Application settings** → **Settings of apps** → **Routing** tab. The following information is displayed for each route in the table:

- **Status** – route activity status (**Active** or **Error**).
- **Source app** – name of the app that sends data.
- **Source connection point** – name of the connection point of the source app.

- **Destination app** – name of the app that receives data.
- **Destination connection point** – name of the connection point of the destination app.

To find a route or configure how data is displayed in the app routing table:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Routing**.
A table displaying the previously created routes for each app will be displayed.
7. If you want to find a route, enter a value in the search field in the upper part of the table and click the **Q** icon or press **ENTER**.
The table will display only the routes matching your search query. If you previously configured data filtering in the app routing table, the search will be performed only for filtered values.
8. If you want to sort data in the table based on one of the columns, click the column header.
9. If you need to customize the display of columns in the table or group identical values within one column, click the **⌵** icon. In the pane that opens on the right on the **Columns** tab, select the check boxes next to the columns whose data should be displayed. On the **Grouping** tab, select the values that you need to group within one column.
10. If you need to configure how the routes of apps are displayed according to specific conditions, click the **∇** icon and use the pane that opens on the right to configure conditions for displaying routes in the table. You can add new conditions or delete existing conditions.

You can also [create](#), [edit](#) or [delete](#) a route for an app.

Creating a route for an app

To create a new route for an app:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings of apps** → **Routing**.

A table displaying the previously created routes for each app will be displayed.

7. Click the **Add** button in the upper part of the table and do the following in the pane that opens on the right:

- a. In the **Source app** drop-down list, select the app from which the data will be sent. The drop-down list displays only [running apps](#).
- b. In the **Source connection point** drop-down list, select the connection point. The data type, data format, and data transfer protocol are determined by the developer in the app manifest.
- c. In the **Destination app** drop-down list, select the app that will receive the data. The drop-down list displays only [running apps](#).
- d. In the **Destination connection point** drop-down list, select the connection point. The data type, data format, and data transfer protocol are determined by the developer in the app manifest.
- e. Click **Save** in the lower part of the pane.

The route for the app will be created and displayed in the table. A new route is created in the active state by default.

8. Click the **Save** button in the lower part of the page.

Editing a route for an app

To edit a route for an app:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.

2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

5. Select the **Application settings** tab.

6. Select **Settings of apps** → **Routing**.

A table displaying the previously created routes for each app will be displayed.

7. Select the check box next to the route that you want to edit.

8. Click the **Edit** button in the upper part of the table and do the following in the pane that opens on the right:

- a. In the **Source app** drop-down list, select the app from which the data will be sent. The drop-down list displays only [running apps](#).

- b. In the **Source connection point** drop-down list, select the connection point. The data type, data format, and data transfer protocol are determined by the developer in the app manifest.
- c. In the **Destination app** drop-down list, select the app that will receive the data. The drop-down list displays only [running apps](#).
- d. In the **Destination connection point** drop-down list, select the connection point. The data type, data format, and data transfer protocol are determined by the developer in the app manifest.
- e. Click **Save** in the lower part of the pane.

The route for the app will be changed and the new data will be displayed in the table.

9. Click the **Save** button in the lower part of the page.

Deleting a route for an app

To delete a route for an app:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device running Kaspersky IoT Secure Gateway 1000. If the device name is not on the list, [add it to the Managed devices](#) group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.
This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings of apps** → **Routing**.
A table displaying the previously created routes for each app will be displayed.
7. Select the check box next to the route that you want to delete.
8. Click the **Delete** button in the upper part of the table and confirm deletion.
The route for the app will be deleted.
9. Click the **Save** button in the lower part of the page.

Contacting Technical Support

If you have any questions about the Kraftway Rubezh-N hardware system or Kaspersky IoT Secure Gateway 1000 and you have not found a solution to the issue in the Kaspersky IoT Secure Gateway 1000 Help Guide, you are advised to contact Aprotect Technical Support by emailing support@aprotech.ru.

To receive additional information about the state of network interfaces and the routing table, you can go to the troubleshooting page at the following address: <Kaspersky IoT Secure Gateway 1000 web address>/troubleshooting.html. Information is displayed on the <Kaspersky IoT Secure Gateway 1000 web address>/troubleshooting.html page only if you have already logged in to the Kaspersky IoT Secure Gateway 1000.

Viewing the Kaspersky IoT Secure Gateway 1000 troubleshooting page

Further information about the Kaspersky IoT Secure Gateway 1000 network interface statuses and routing table is available on the troubleshooting page.

To go to the troubleshooting page:

In the menu in the left part of the web interface, select **Settings** → **Diagnostics** and click the link.

The <Kaspersky IoT Secure Gateway 1000 web address>/troubleshooting.html page opens.

The troubleshooting page displays the following information:

- [Operating mode of network components \(enabled or disabled\)](#) 

- Masquerading.
- IP forwarding.
- DHCP server.
- DHCP client.

- [Memory state of the embedded computer](#) 

- Number of running processes
- CPU utilization
- Memory usage
- Table of running processes:
 - ID
 - Priority
 - Number of threads
 - Reserved memory size
 - Actually used memory
 - Status
 - Running time
 - CPU breakdown by running process
 - Names of process components and entities

- [Kaspersky IoT Secure Gateway 1000 network interface information](#)

- Interface name.
- MAC address.
- IP address.
- Broadcast address.
- Subnet mask.
- Broadcast address operating mode.
- Maximum size of the data payload of one packet.
- Number of received and sent network packets:
 - If Kaspersky IoT Secure Gateway 1000 is running as a network router device, information for the interfaces of the external network and internal network, local device, and network tunnel is displayed.
 - If Kaspersky IoT Secure Gateway 1000 is running as unidirectional gateway device, information about the interfaces of the external network, local device, and network tunnel is displayed.

- [Kaspersky IoT Secure Gateway 1000 routing table information](#)

- Route status (active or error).
- Route type (static or dynamic).
- Destination IP address.
- Destination network mask.
- Gateway.
- Error code (if the route status is "error").

- [Information about Kaspersky IoT Secure Gateway 1000 firewall rules](#)

- System firewall rules.
- Custom firewall rules.
- Kaspersky IoT Secure Gateway Network Protector application rules.

- [Information about address translation rules](#)

- Network interface to which the rule applies.
- External port.
- Protocol.
- Destination IP address.
- Port of the destination node.
- Comment.

Information about the address translation rules is displayed only for the [network router device type](#).

- [Information about the network cluster](#)

- Cluster IP address.
- Cluster IP address mask.
- Role of a device in a cluster.

You can also do the following on the troubleshooting page:

- [Download an archive file containing the Kaspersky IoT Secure Gateway 1000 system log](#)

On the troubleshooting page at <Kaspersky IoT Secure Gateway 1000 web address>/troubleshooting.html, click **Download system logs**.

The archive containing the Kaspersky IoT Secure Gateway 1000 system log will begin downloading automatically.

- [Check the device network access \(ping\)](#)

1. On the troubleshooting page at <Kaspersky IoT Secure Gateway 1000 web address>/troubleshooting.html, in the **Check connection via ping command** form, enter the DNS name or IP address of the device whose network access you want to verify.

2. Click **Submit**.

Under the form below, information on the verification results will be displayed (for example, the size and number of sent packets, packet transit time, and lost packet statistics).

Kaspersky IoT Secure Gateway 1000 does not provide the capability to define keys for the command to verify network access of a device IP address or DNS name.

Additional Information

This section provides additional information to supplement the primary text of the document.

Preparing to install Kaspersky IoT Secure Gateway 1000

Before installing Kaspersky IoT Secure Gateway 1000, you have to prepare the Kraftway Rubezh-N device for installation.

[Preparations for Kaspersky IoT Secure Gateway 1000 installation](#) are performed by Kaspersky experts. The instructions described in this section are provided for information purposes.

Preparing the Kraftway Rubezh-N device

To prepare the Kraftway Rubezh-N device for installing Kaspersky IoT Secure Gateway 1000:

1. [Turn on the Kraftway Rubezh-N device.](#)
2. Connect the Kraftway Rubezh-N device through a COM port to a local computer using a cable with an RJ45-DB9 connector.
Connect the cable to the Kraftway Rubezh-N device console connector.
3. On the local computer, start a COM port terminal application, such as PuTTY or Minicom.
4. Click the on/off button in the left part of the Kraftway Rubezh-N front panel.
The power indicator will light up on the front panel of Kraftway Rubezh-N, and the device will start running.
5. While the device is loading, press the **DELETE** key on the keyboard.
The main BIOS menu of the Kraftway Rubezh-N device opens in the terminal.
6. Check the date and time settings.
 - a. Select the **Main** tab.
 - b. Select **System Date**. If necessary, indicate the correct date.
 - c. Select **System Time**. If necessary, indicate the correct time.
7. Exit BIOS while saving the changes:
 - a. Select the **Save & Exit** tab.
 - b. On the **Save & Exit** tab, select **Save Changes & Exit**.

Kraftway Rubezh-N will reboot with the configured settings. The device will continue to start with the configured settings on subsequent startups. Before installing Kaspersky IoT Secure Gateway 1000, the device must be shut down.

Installing Kaspersky IoT Secure Gateway 1000

To get started with Kaspersky IoT Secure Gateway 1000, install it on the Kraftway Rubezh-N device.

[Installation of Kaspersky IoT Secure Gateway 1000](#) is performed by Kaspersky experts. The instructions described in this section are provided for information purposes.

To install Kaspersky IoT Secure Gateway 1000:

1. Prepare a computer with Ubuntu version 20.04 or later for creating bootable USB drive with the Kaspersky IoT Secure Gateway 1000 image. All further actions must be performed on this computer.
2. Install the `wget` and `sha512sum` utilities by running the following command as root:

```
sudo apt-get install wget coreutils
```

3. Add the `docker` repository PGP™ key to the system by running the following commands as root:

```
sudo apt-get update
sudo apt-get install ca-certificates curl gnupg
sudo install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

4. Add the `docker` repository address to the system by running the following commands:

```
echo \
"deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
"${(. /etc/os-release && echo "$VERSION_CODENAME")}" stable" | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

5. Update package data and install `docker` by running the following commands as root:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

6. Prepare `docker` to run with user permissions by executing the following commands as root:

```
sudo groupadd docker
sudo usermod -aG docker <system user name>
newgrp docker
```

7. Verify that `docker` starts without errors by running the test image:

```
docker run hello-world
```

8. Connect a USB drive containing the `flasher` utility with a boot image script to your computer and copy it to a separate directory.

9. Go to the directory that contains the `flasher` utility.

10. Copy the Kaspersky IoT Secure Gateway 1000 firmware image to the `resources` directory. The image must have a name in the format `kisg-<network device type>-<system version number>_ru_en.tar.gz`, where `<network device type>` can be `diode` for unidirectional gateway or `router` for a network router, and `<system version number>` consists of four decimal numbers separated by dots, such as `1.2.3.4`.

You can place one installation image in the directory if you intend to use one type of network device only, or both installation images (for unidirectional gateway and network router) to be able to choose between the types of network device when installing Kaspersky IoT Secure Gateway 1000.

11. Edit the `flasher.conf` configuration file, so that it contains only the following lines:

```
set -eu
KISG_images=()
KISG_device=kraftway
```

12. Verify that the `wget` utility can download a Debian OS image by running the following command:

```
wget https://www.debian.org/CD/
```

If the `wget` utility fails to get the Debian OS image, place the [Debian 11.4.0 image](#) and [SHA512 checksums](#) into the `resources` directory

<https://get.debian.org/images/archive/11.4.0-live/amd64/iso-hybrid/debian-live-11.4.0-amd64-standard.iso>
. If there is no Internet connection on the computer with the `flasher` utility, obtain a Debian docker image by running `docker pull debian: bullseye` and copy the resulting image to the `flasher` utility directory.

13. Build the boot image of Kaspersky IoT Secure Gateway 1000 by running the build script using the following command:

```
./build.sh
```

14. Make sure that the boot image of Kaspersky IoT Secure Gateway 1000 is built successfully by running the following command:

```
file KISGFlasher.iso
```

15. Connect a new USB drive to the computer with the `flasher` utility.

16. Write the Kaspersky IoT Secure Gateway 1000 boot image to the USB drive by running the following command with root privileges:

```
dd bs=4M if=$(pwd)/KISGFlasher.iso of=/dev/sdx status=progress oflag=sync
```

where `/dev/sdx` is the name of the USB drive to which you need to write the image.

17. Wait for the writing process to complete successfully and remove the USB drive.
18. Connect the USB drive to the Kraftway Rubezh-N device.
19. Connect the Kraftway Rubezh-N device through a COM port to a local computer using a cable with an RJ45-DB9 connector and start a COM port terminal application on the local computer.
All further actions must be performed in the terminal of the computer connected to the Kraftway Rubezh-N device.
20. Click the on/off button in the left part of the Kraftway Rubezh-N front panel.
21. While the device is starting, press **DELETE** on the console keyboard.
The main BIOS menu of the Kraftway Rubezh-N device opens in the console.
22. Configure the settings for loading Kaspersky IoT Secure Gateway 1000 from a bootable USB drive:
 - a. Select the **Save & Exit** tab.
 - b. In the **Boot Override** section, use the \uparrow and \downarrow keys to select **UEFI: <name of bootable USB drive>**.
 - c. Press **ENTER** to start booting from the USB drive.
23. Wait for the image to load from the USB drive.
24. In the `debian login` form that appears in the console, enter the default Debian Live CD user name and password to log in to LiveUSB.
25. If you have compiled a boot image for two network device types, select from the menu the Kaspersky IoT Secure Gateway 1000 image to install on the device (unidirectional gateway and network router) and press **ENTER**.
If you have compiled a boot image for one network device type only, installation starts automatically.
26. Wait for the installation process to complete. After installation, the Kraftway Rubezh-N device shuts down.
27. Remove the USB drive from the Kraftway Rubezh-N device.
28. Click the on/off button in the left part of the Kraftway Rubezh-N front panel.
29. While the device is starting, press **DELETE** on the console keyboard.
The main BIOS menu of the Kraftway Rubezh-N device opens in the console.
30. Configure the boot order for Kaspersky IoT Secure Gateway 1000:
 - a. Select the **Boot** tab.
 - b. For **Boot Option # 1**, select **UEFI OS**.

31. Exit BIOS while saving the changes:

- a. Select the **Save & Exit** tab.
- b. On the **Save & Exit** tab, select **Save Changes & Exit**.

32. Wait for the download to complete and visually check that Kaspersky IoT Secure Gateway 1000 starts correctly.

After Kaspersky IoT Secure Gateway 1000 starts for the first time, it is recommended to [configure the network](#), [create and upload an administrator certificate](#), [configure the date and time](#), and [replace the web server certificate](#) with the one that is used in your organization.

Error connecting to the Kaspersky IoT Secure Gateway 1000 web interface

Issue

When connecting to the Kaspersky IoT Secure Gateway 1000 web interface using the [supported](#) Google Chrome web browser, the login page for the Kaspersky IoT Secure Gateway 1000 web interface does not load.

Solution

To successfully connect to the Kaspersky IoT Secure Gateway 1000 web interface using the Google Chrome web browser, your operating system must use the standard system port range for TCP connections.

Some applications that may be installed on your personal computer running a Windows® operating system may have changed the default system port range that is used to connect over the TCP protocol.

To successfully connect to the Kaspersky IoT Secure Gateway 1000 web interface using the Google Chrome web browser:

1. Open a console on the computer where you are trying to connect to the Kaspersky IoT Secure Gateway 1000 web interface.
2. In the console run the following command, which will display the range ports that are used by the system for TCP protocol connection:

```
netsh int ipv4 show dynamicport tcp
```

The console will display the port range used for the TCP protocol.

3. If the displayed port range starts with port 1024, then run the following command as an administrator to restore the system port range for the TCP protocol to its default values:

```
netsh int ipv4 set dynamicport tcp start=49152 num=16384
```

4. Try again [to connect to the Kaspersky IoT Secure Gateway 1000 web interface](#) using the Google Chrome browser.

The Kaspersky IoT Secure Gateway 1000 login page opens.

Glossary

Administration Server

A Kaspersky Security Center entity that centrally stores information about all Kaspersky applications that are installed within an enterprise network. It can also be used to manage these applications.

Administrator certificate

A certificate used for user authentication in the Kaspersky IoT Secure Gateway 1000 web interface.

Application administration plug-in

A specialized entity that provides an interface for application management through the Administration Console. Each application has its own administration plug-in. It is included in all Kaspersky applications that can be managed using Kaspersky IoT Secure Gateway 1000.

Event

A record containing information about detecting data in the system or on the LAN that requires the attention of an employee responsible for data security in your organization. An event is stored in the memory of the Kraftway Rubezh-N embedded computer.

Internet of Things (IoT)

A network of interrelated electronic devices (things) that are equipped with built-in capabilities for interaction with the external environment or with each other without human involvement.

Internet of Things (IoT) Secure Gateway

A system that ensures secure transmission of user traffic between sensors and an IoT platform.

Kaspersky IoT Secure Gateway 1000 entity

A part of Kaspersky IoT Secure Gateway 1000 that is designed to provide system functionality (such as authentication).

Kaspersky Security Center 14.2 Web Console

A web application designed to manage the state of the security system of enterprise networks that are protected by Kaspersky applications.

Kaspersky Security Center administrator

The person who manages application operations through the remote centralized administration system known as Kaspersky Security Center.

KasperskyOS

A microkernel operating system used for building secure solutions.

KSC server certificate

A certificate that is used for secure interaction between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center when managing Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 14.2 Web Console.

Managed devices

Enterprise network devices that are included into an administration group.

Message Queuing Telemetry Transport (MQTT)

A network protocol that works on top of the TCP/IP protocol stack to exchange messages between devices on the Internet of Things.

MQTT broker

A server that receives, filters, and forwards messages over the MQTT protocol.

MQTT-topic

A hierarchical path to the data source used for sending messages over the MQTT protocol.

SSL

A protocol for data encryption in local networks and on the Internet. SSL is used in web applications to create secure connections between a client and a server.

TLS

Secure protocol that uses encryption to transfer data in local networks and on the Internet. TLS is used in web applications to create secure connections between a client and a server.

UEFI protection device

A device with Kaspersky Anti-Virus for UEFI integrated at the BIOS level. Integrated protection ensures device security from the moment the system starts. In contrast, devices without integrated software are protected only after the security application starts.

Information about third-party code

Information about third-party code is contained in the file named `legal_notices.txt`, which is located on the local web server. You can open the file from the **About** section.

Trademark notices

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

Ubuntu is a registered trademark of Canonical Ltd.

Eclipse Mosquitto is a trademark of Eclipse Foundation, Inc.

Google and Google Chrome are trademarks of Google LLC.

HUAWEI is a trademark of Huawei Technologies Co., Ltd.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Kraftway is a registered trademark of Kraftway Corporation PLC.

OpenAPI is a trademark of The Linux Foundation.

Windows is a trademark of Microsoft group of companies.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the U.S. and other countries.

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

OpenSSL is a trademark owned by the OpenSSL Software Foundation.

Debian is a registered trademark of Software in the Public Interest, Inc.

PGP is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.