



kaspersky

Kaspersky IoT Secure Gateway

© 2020 AO Kaspersky Lab

Contents

[About Kaspersky IoT Secure Gateway](#)

[Distribution kit](#)

[Hardware and software requirements](#)

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

[Components of Kaspersky IoT Secure Gateway](#)

[Preparing to install Kaspersky IoT Secure Gateway](#)

[Installing Kaspersky IoT Secure Gateway](#)

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

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

[Kaspersky IoT Secure Gateway web interface](#)

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

[Dashboard section](#)

[Events section](#)

[Audit section](#)

[Devices section](#)

[MQTT broker section](#)

[Settings section](#)

[Network settings block](#)

[System security settings block](#)

[Web server settings block](#)

[Utilities settings block](#)

[General settings block](#)

[KSC settings block](#)

[About section](#)

[User menu](#)

[Data provision](#)

[Licensing Kaspersky IoT Secure Gateway](#)

[Configuring Kaspersky IoT Secure Gateway](#)

[Configuring network settings](#)

[Managing the password policy](#)

[Changing a user password](#)

[Configuring MQTT broker settings](#)

[Creating a new MQTT broker profile](#)

[Completing an empty MQTT broker profile](#)

[Modifying an MQTT broker profile](#)

[Switching to a different MQTT broker profile](#)

[Limitations when configuring an MQTT broker](#)

[Configuring the web server](#)

[Creating a new web server profile](#)

[Completing an empty web server profile](#)

[Modifying the web server profile](#)

[Switching to a different web server profile](#)

[Configuring the date and time](#)

[Monitoring devices](#)

[Monitoring events](#)

[Viewing the network security log](#)

[Viewing the audit log](#)

[Forwarding event logs to a Syslog server](#)

[Forwarding push notifications](#)

[Forwarding MQTT notifications](#)

[Intrusion Detection](#)

[Monitoring the state of Kaspersky IoT Secure Gateway](#)

[Viewing information about system users](#)

[Viewing the state of components](#)

[Managing the application through the Kaspersky Security Center Web Console](#)

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

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

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

[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)

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

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

[Creating a new MQTT broker profile through the Kaspersky Security Center Web Console](#)

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

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

[Configuring network settings through the Kaspersky Security Center Web Console](#)

[Managing the firewall](#)

[About firewall rules](#)

[Creating firewall rules](#)

[Editing firewall rules](#)

[Changing the order of firewall rules](#)

[Deleting firewall rules](#)

[Managing the Intrusion Prevention system](#)

[Procedure for processing network traffic](#)

[Managing the web server through the Kaspersky Security Center Web Console](#)

[Configuring Syslog](#)

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

[Configuring the date and time](#)

[Configuring a password policy](#)

[Configuring synchronization with Kaspersky Security Center](#)

[Configuring masquerading](#)

[Restarting and updating software](#)

[Contacting Technical Support](#)

[Glossary](#)

[Event](#)

[Internet of Things \(IoT\)](#)

[Internet of Things \(IoT\) Secure Gateway](#)

[Kaspersky IoT Secure Gateway entity](#)

[Kaspersky Security Center Web Console](#)

[KasperskyOS](#)

[Message Queuing Telemetry Transport \(MQTT\)](#)

[MQTT broker](#)

[MQTT-topic](#)

[Password policy](#)

[Information about third-party code](#)

Trademark notices

About Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway (hereinafter also referred to as "the system") consists of the KasperskyOS operating system with a preconfigured set of application software. Kaspersky IoT Secure Gateway is intended for installation on a built-in Advantech UTX-3117-S6A1N computer.

The Kaspersky IoT Secure Gateway system is designed to serve as a secure gateway for the Internet of Things in an enterprise network.

System version: Kaspersky IoT Secure Gateway 2.0 Beta

Kaspersky IoT Secure Gateway 2.0 Beta is distributed solely to conduct testing in the information and communication environment used in legal entities.

Kaspersky IoT Secure Gateway performs the following functions:

- Receives, scans, and distributes messages of sensors and other devices transmitted over the MQTT protocol.
- Registers security events of the system and network.
- Detects devices within the internal enterprise network.
- Detects attempts of intrusion into the internal enterprise network.
- Ensures the cybersecurity of the device itself and provides methods for controlling connected devices.

Kaspersky IoT Secure Gateway can also operate as a firewall and DHCP server, and provide network address translation (NAT).

You can manage Kaspersky IoT Secure Gateway through the local web interface or remotely by using the web plug-in for the Kaspersky Security Center Web Console.

Distribution kit

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

- Installation image for Kaspersky IoT Secure Gateway: kisg-<application version number>-ru-en.tgz.
- Archive containing the installation image for the Kaspersky Security Center Web Console web plug-in and signature file: WEB_Plugin_KISG_<plug-in version number>.zip.
- File containing information about third-party code (Legal Notices).
- Online documentation.
- Version information (Release Notes).

Hardware and software requirements

The Kaspersky IoT Secure Gateway system can be installed only to the built-in computer Advantech UTX-3117FS-S6A1N.

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

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

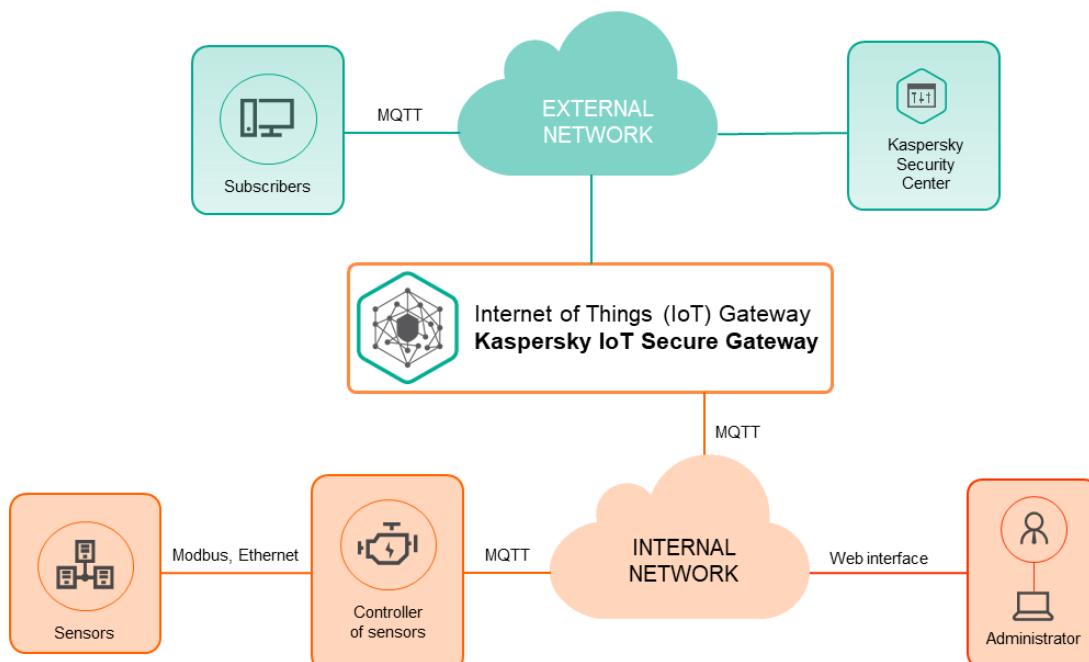
- Google Chrome™ version 76 or later.
- Mozilla™ Firefox™ version 68 or later.

Standard deployment of Kaspersky IoT Secure Gateway

The standard deployment scenario for Kaspersky IoT Secure Gateway (see the figure below) involves the following:

1. Sensors transmit telemetry data (for example, over the Modbus protocol) to the sensor controller.
2. The sensor controller publishes measurement data in the form of MQTT-topics to the internal network.
3. Kaspersky IoT Secure Gateway receives MQTT-topics and transmits them to subscribers in the external network. Data acquisition and visualization servers normally act as the subscribers.

An administrator can manage the system and track its state from the internal network through the web interface and via the Kaspersky Security Center server.



Standard deployment of Kaspersky IoT Secure Gateway

Components of Kaspersky IoT Secure Gateway

Kaspersky IoT Secure Gateway includes the following components:

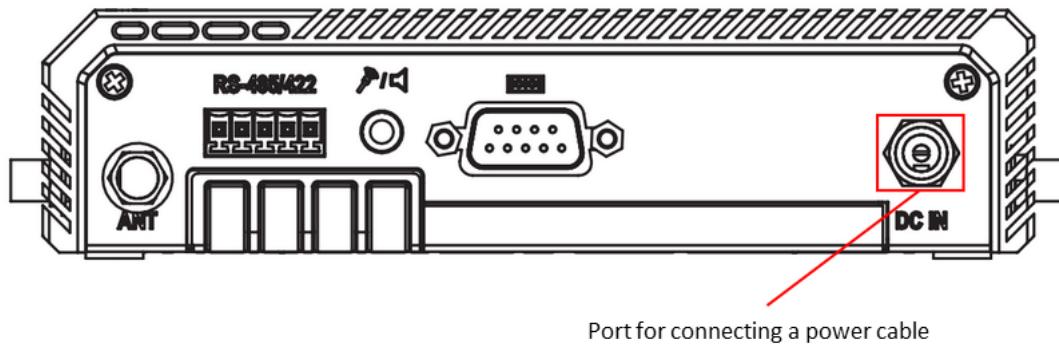
- *Secure manager*. Facilitates data exchange between components of Kaspersky IoT Secure Gateway, and serves as the point for receiving information about the security state of other components.
- *Auth server*. Provides user account authentication (asks the *Secure storage* component for password verification data).
- *Traffic processor*. Provides the functionality for detecting devices on the network and supports the authorized list of devices.
- *Secure storage*. Used to store public keys of certificates and system user accounts.
- *Config manager*. Used to store the configuration parameters of all system components.
- *Traffic controller*. Supports operation of the network interfaces of the system.
- *Web server*. Supports operation of the web interface of the system.
- *MQTT broker*. Provides MQTT broker functionality.
- *Blocker*. Blocks nodes whose malicious activity is detected by the IDS component.
- *IPS*. Provides Intrusion Prevention functionality.
- *Logger*. Stores debug logs of the system.
- *Tee manager*. Monitors the operating state of all system components.
- *Bootloader*. Ensures that the system software is securely loaded.
- *Firewall*. Provides firewall and connection control functionality.
- *KSC controller*. Provides a connection to the centralized management system Kaspersky Security Center.

Preparing to install Kaspersky IoT Secure Gateway

Prior to installing Kaspersky IoT Secure Gateway, you need to configure the Advantech UTX-3117FS-S6A1N.

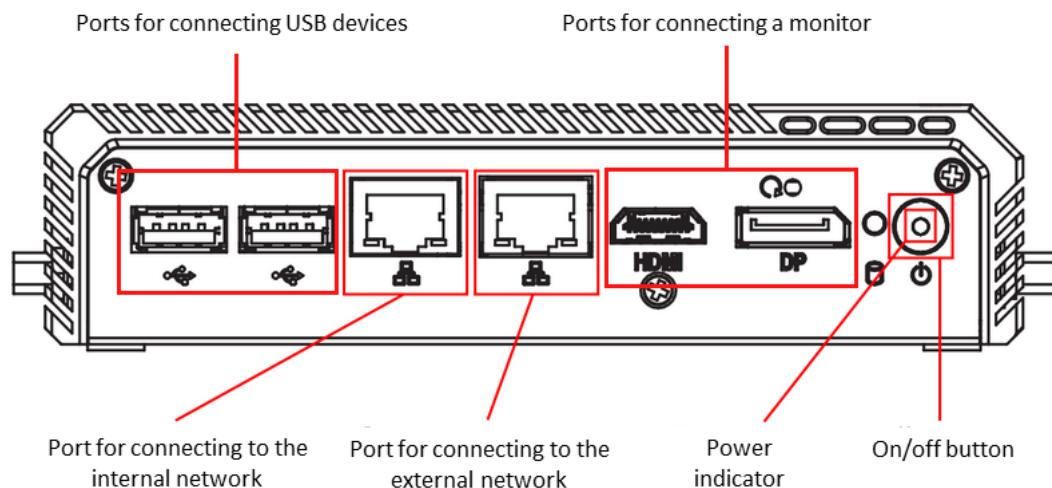
To configure the Advantech UTX-3117FS-S6A1N:

1. Connect a power cable to the port on the back panel of the Advantech UTX-3117FS-S6A1N (see the figure below).



Back panel of the Advantech UTX-3117FS-S6A1N

2. Connect the network cable for the external network to the port on the front panel of the Advantech UTX-3117FS-S6A1N (see the figure below).



Front panel of the Advantech UTX-3117

3. Connect a monitor and keyboard to the appropriate ports on the front panel of the Advantech UTX-3117FS-S6A1N.

4. Click the on/off button in the right part of the front panel of the Advantech UTX-3117.

The power indicator will light up on the front panel of the Advantech UTX-3117 and the system will start running.

5. Press the **DELETE** key.

The main BIOS menu opens.

6. Restore the default settings:

- a. Select the **Save & Exit** tab.

- b. In the **Default Options** menu, select **Restore Defaults**.
 - c. Exit the **Save & Exit** tab.
7. Check the Secure Boot settings:
- a. Select the **Security** tab.
 - b. Select **Secure Boot**.
 - c. Make sure that the **Secure Boot** parameter is **Not Active**:
 - If **Secure Boot** is **Not Active**, proceed to the next step.
 - If **Secure Boot** is **Active**, change it to **Not Active** and restart the Advantech UTX-3117FS-S6A1N.
 - d. Exit the **Security** tab.
8. Configure the southbridge:
- a. Select the **Chipset** tab.
 - b. In the opened menu, select **South Bridge**.
 - c. For the **OS Selection** setting value, select **Intel Linux**.
 - d. Exit the **Chipset** tab.
9. Configure the advanced settings:
- a. Select the **Advanced** tab.
 - b. In the opened menu, select **CSM Configuration**.
 - c. For the **CSM Support** setting value, select **Enabled**.
 - d. For the **Network and Other PCI devices Support** setting values, select **Do not launch**.
 - e. Return to the **Advanced** tab.
 - f. In the opened menu, select **CPU Configuration**. For the **VT-d** setting value, select **Enabled**.
 - g. Return to the **Advanced** tab.
 - h. In the opened menu, select **Serial Port Console Redirection**.
 - i. For the **Console Redirection** setting value, select **Enabled**.
 - j. Select **Console Redirection Settings**.
 - k. For the **Terminal Type** setting value, select **VT100+**.
 - l. Exit the **Advanced** tab.
10. Configure the boot settings:

- a. Select the **Boot** tab.
- b. For the **Boot Option #1** setting value, select **UEFI: Build-in EFI shell**.
- c. Exit the **Boot** tab.

11. Exit BIOS while saving the changes:

- a. Select the **Save & Exit** tab.
- b. On the **Save & Exit** tab, select **Save Changes & Exit**.

Installing Kaspersky IoT Secure Gateway

To install Kaspersky IoT Secure Gateway:

1. Download the SystemRescueCd distribution package image from the official website.
2. Create a bootable USB drive containing the SystemRescueCd distribution package, for example, by using the dd utility:

```
$ dd if=systemrescued-6.0.3.iso of=/dev/%USB device name%
```
3. Insert the bootable USB drive containing the SystemRescueCd distribution package into the USB port on the Advantech UTX-3117FS-S6A1N.
4. Click the on/off button in the right part of the front panel of the Advantech UTX-3117.
SystemRescueCd loads automatically.
5. Go to the directory /tmp by entering the following command in the command line:

```
$ cd /tmp
```
6. Download the Kaspersky IoT Secure Gateway installation image from the network, for example, by using the wget utility:

```
$ wget %path to the installation image of Kaspersky IoT Secure Gateway%
```
7. Use the command line to unpack the image:

```
$ tar -xzf latest-kos-mqtt-broker.tgz  
$ cd kos-mqtt-broker/install  
$ tar -xzf install.tar.gz
```
8. Start the installation:

```
$ ./install.sh
```
9. When installation completes, use the SystemRescueCd tools to restart the Advantech UTX-3117FS-S6A1N.
10. Eject the bootable USB drive containing the SystemRescueCd distribution package.

After the restart, Kaspersky IoT Secure Gateway starts automatically.

After it starts for the first time, it is recommended to [configure the network](#), [change the default administrator password](#), [configure the date and time](#), and [replace the web server certificate](#) with the one that is used in your organization.

Connecting to the Kaspersky IoT Secure Gateway web interface

You can connect to the Kaspersky IoT Secure Gateway web interface using any [supported browser](#). The browser must be installed on a computer that has access to Kaspersky IoT Secure Gateway through the internal network.

The Kaspersky IoT Secure Gateway system is delivered with a statically configured IP address. To connect to the system and perform initial configuration, you need to configure your computer to have an IP address within the same network as Kaspersky IoT Secure Gateway. You can find out the IP address of Kaspersky IoT Secure Gateway by contacting Kaspersky Technical Support experts.

To connect to the Kaspersky IoT Secure Gateway web interface:

1. Open your browser.
2. In your browser's address bar, enter the IP address.

The account credentials entry page opens.



kaspersky

© 2020 AO Kaspersky Lab

Account credentials entry page in the browser window

3. In the **User name** field, enter the user name.
4. In the **Password** field, enter the password.
5. Click the **Log in** button.

The browser window will display the Kaspersky IoT Secure Gateway web interface page.

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

For security purposes, Kaspersky IoT Secure Gateway 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 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 10 minutes. During this time, the system can grant access to the Kaspersky IoT Secure Gateway web interface without prompting for user account credentials, provided that the connection uses the same computer and browser.

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

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

The user menu appears.

2. In the user menu, select **Log out**.

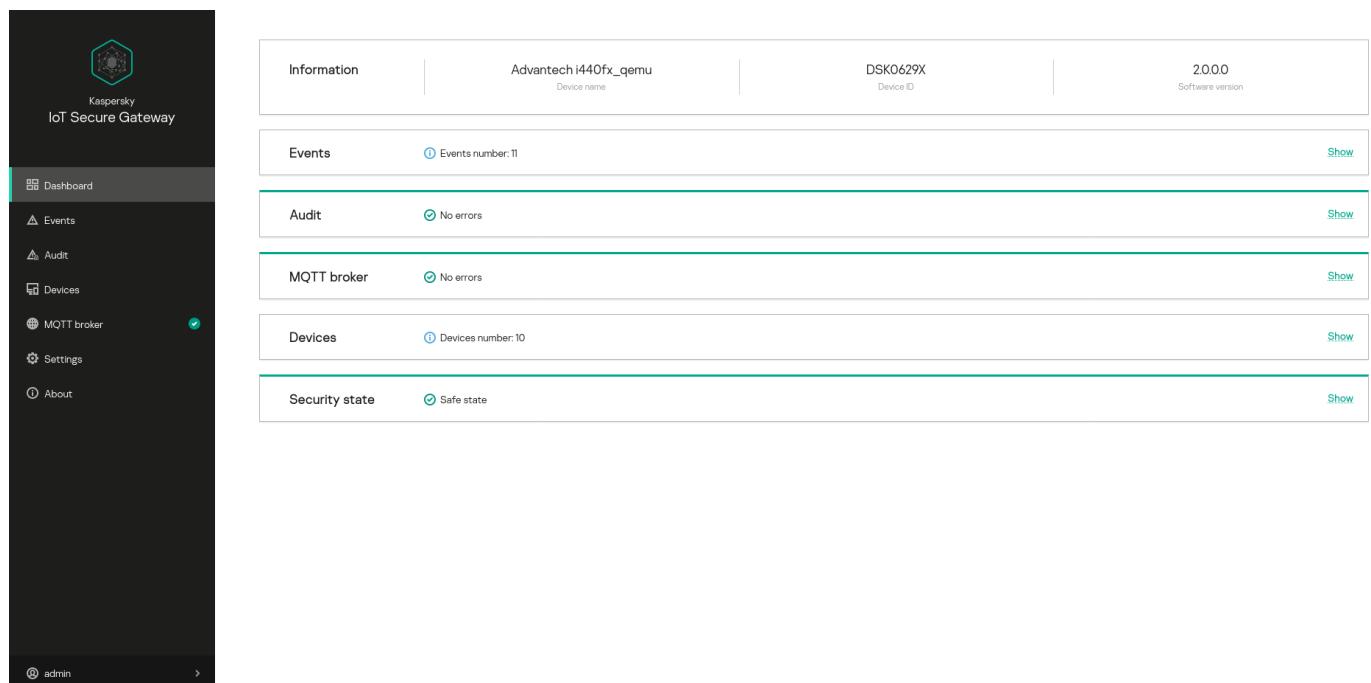
The browser window shows the page for entering account credentials.

Kaspersky IoT Secure Gateway web interface

This section describes the main elements of the Kaspersky IoT Secure Gateway web interface.

Kaspersky IoT Secure Gateway web interface menu

The menu is displayed in the left part of the Kaspersky IoT Secure Gateway web interface page. The contents of the section selected in the menu are displayed on the right (see the figure below).



The screenshot shows the Kaspersky IoT Secure Gateway web interface. On the left, there is a dark sidebar with the Kaspersky logo and the text "Kaspersky IoT Secure Gateway". Below the logo are several menu items: "Dashboard" (selected), "Events", "Audit", "Devices", "MQTT broker" (selected), "Settings", and "About". At the bottom of the sidebar are user information ("admin") and navigation icons. The main content area on the right displays the "MQTT broker" section. It includes a header with "Information" (Device name: Advantech i440fx_qemu, Device ID: DSK0629X, Software version: 2.0.0), followed by five cards: "Events" (Events number: 11, Show), "Audit" (No errors, Show), "MQTT broker" (No errors, Show), "Devices" (Devices number: 10, Show), and "Security state" (Safe state, Show). Each card has a "Show" link at the end.

Page of the application web interface in the browser window

The web interface menu contains the following sections:

	<u>Dashboard</u> Opens the section containing information about the latest events, detected devices, and the state of system components.		<u>Events</u> Opens the section displaying network security events.
	<u>Audit</u> Opens the section displaying system security events.		<u>Devices</u> Opens the section displaying the devices detected in the network.
	<u>MQTT broker</u> Opens the section that displays MQTT broker profiles.		<u>Settings</u> Opens the section in which you can view and change the system settings.
	<u>About</u> Opens the section containing concise information about the system.		<u><User name></u> Expands or collapses the user menu.

Dashboard section

In the **Dashboard** section (see the figure below), you can view consolidated information about the system.

The screenshot shows the Kaspersky IoT Secure Gateway dashboard. The left sidebar has a dark theme with white icons and text. The 'MQTT broker' item is highlighted with a green checkmark. The main area is titled 'Dashboard' and contains several status cards:

- Information:** Device name: Advantech i440fx_gemu, Device ID: DSK0629X, Software version: 2.0.00
- Events:** Events number: 11, [Show](#)
- Audit:** No errors, [Show](#)
- MQTT broker:** No errors, [Show](#)
- Devices:** Devices number: 10, [Show](#)
- Security state:** Safe state, [Show](#)

Dashboard section

The **Dashboard** section displays the following information blocks:

- **Information** – the name and serial number of the hardware platform, and the Kaspersky IoT Secure Gateway system version.
- **Events** – the number of network security events. If you expand the **Events** block by clicking the **Show** link, you will see the number of network security events for each component that registered events.

Network security events are not stored in the system and are available only while the current session of the web interface connection is active.

- **Audit** – information about the presence of system security events that are written to the audit log. If the system has registered events with the *Warning* or *Critical* severity level, the block shows **Issues**. If there are no events with the *Warning* or *Critical* severity level, the block shows **No errors**. Click the **Show** link to expand the **Audit** block to view the number of system security events for each severity level.
- **MQTT broker** – statistics of system operation over the MQTT protocol. If the system has detected problems with data transfer over the MQTT protocol, the block shows **Issues**. If there are no problems with data transfer over the MQTT protocol, the block shows **No errors**.
- **Devices** – the number of devices [detected in the network](#).
- **Security state** – status of the security of system [components](#).

Events section

In the **Events** section (see the figure below), you can view network security events that occurred during the current session of the user's connection to the system through a browser. Network security events include the appearance and disappearance of devices in the network, and attempts by a device to connect to the web interface.

The screenshot shows the Kaspersky IoT Secure Gateway interface. On the left is a dark sidebar with navigation links: Dashboard, Events (which is selected and highlighted in blue), Audit, Devices, MQTT broker, Settings, and About. At the bottom of the sidebar are user information (admin) and a log out button. The main content area has a title 'Network security events'. Below it is a toolbar with a 'Entity' dropdown set to 'Auth server', a 'Text' dropdown set to 'Unknown device', and a 'Date and time' dropdown. There is also an 'Auto-update table' toggle button. The main part of the screen is a table with the following columns: Entity, Event, Text, and Date and time. The table lists 15 rows of events, all from the 'Traffic processor' component, all of which are 'Unknown device' events, all occurring at 22/04/2020 16:24:00, and all with a redacted 'Text' field. The last row is timestamped at 22/04/2020 16:23:54.

Entity	Event	Text	Date and time
Auth server	Login successful	User 'admin' logged in successfully	22/04/2020 16:24:40
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:35
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:35
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:35
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:25
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:25
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:15
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:15
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:04
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:04
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:04
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:04
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:24:04
Traffic processor	Unknown device	Detected unknown device with MAC address [REDACTED]	22/04/2020 16:23:54

Events section

The upper part of the **Events** section has a toolbar containing the following elements for managing the table of network security events:

- **Auto-update table** – enables automatic update of event log entries on the page. If the **Auto-update table** toggle button is switched off, the page displays only those events that were in the log when the **Network security events** section was opened.
- **Entity** – groups buttons for enabling and disabling event filtering based on the component that registered the event: *Auth server*, *Traffic processor*.

The following information is displayed for each entry of the network security event log:

- **Entity** – name of the component that registered the event.
- **Event** – type of event.
- **Title** – information about the event.
- **Date and time** – date and time when the event occurred.

Audit section

In the **Audit** section (see the figure below), you can [view the audit log](#) where system security events are stored.

Severity	Title	Entity	Date and time
Informational	SM: All secure entities started and running	Secure manager	22/04/2020 16:23:11
Informational	SM: All secure entities started and running	Secure manager	22/04/2020 16:15:31
Informational	SM: All secure entities started and running	Secure manager	22/04/2020 15:58:21
Informational	SM: All secure entities started and running	Secure manager	22/04/2020 14:08:32

Audit section

The upper part of the **Audit** section has an ⓘ icon that lets you receive information about the audit settings, and a toolbar that contains the following elements for managing the system security events table:

- **Download All** – lets you upload an audit log from the system to the administrator's computer.

Downloading an audit log will result in its deletion from the system.

- **Auto-update table** – enables automatic update of event log entries on the page. If the **Auto-update table** toggle button is switched off, the page displays only those events that were in the audit log when the **Audit** section was opened.
- **Severity** – groups buttons for enabling and disabling event filtering based on severity level: ⓘ *Informational*, ⚠ *Warning*, and ⚡ *Critical*.
- **Period** – lets you select the period for displaying events:
 - **All** – for the entire operating time of the device.
 - **Last day** – during the past 24 hours.
 - **Last week** – during the past week.
 - **Last month** – during the past month.

The following information is displayed for each audit log entry:

- ⓘ – severity of the event.
- **Title** – information about the event.
- **Entity** – name of the component that registered the event.
- **Date and time** – date and time when the event occurred.

Devices section

In the **Devices** section (see the figure below), you can view a table of devices detected within the internal network, add trusted devices to the trusted list, and delete devices from the trusted list.

The application automatically removes the device from the table of detected devices if this device is not present on the network for three minutes.

The screenshot shows the Kaspersky IoT Secure Gateway interface. On the left is a sidebar with the following items:

- Dashboard
- Events
- Audit
- Devices** (selected)
- MQTT broker
- Settings
- About

The main area is titled "Devices" and contains a toolbar with the following elements:

- Whitelist (toggle button)
- Type (dropdown menu set to "Unknown device")
- Workstation (dropdown menu)
- Update (button)

Below the toolbar is a table with the following columns:

Name	Type	Status	MAC address	IP address	Details
device1	Unknown device	Authorized	[REDACTED]	[REDACTED]	...
device2	Unknown device	Authorized	[REDACTED]	[REDACTED]	...
device3	Unknown device	Authorized	[REDACTED]	[REDACTED]	...
device4	Unknown device	Authorized	[REDACTED]	[REDACTED]	...

Devices section

The upper part of the **Devices** section has a toolbar containing the following elements for managing the devices table:

- **Update** – lets you refresh the list of detected devices.
- **Allowlist** lets you display all unauthorized devices in the network (if the toggle button is switched off) or only the devices that are on the authorized list (if the toggle button is switched on).
- **Type** – lets you display all devices of one type.

The following information is displayed for each device:

- **Name** – name of the device.
- **Type** – type of device.
- **Status** – status of the device.
- **MAC address** – MAC address of the device.
- **IP address** – IP address of the device.
- **Details** – operating system and vendor of the device (if identified).

MQTT broker section

In the **MQTT broker** section (see the figure below), you can view and [change the MQTT broker settings](#).

Depending on whether the MQTT broker settings have been correctly configured in the menu next to the **MQTT broker** item, one of the following badges will be displayed:

- Icon . This means that the MQTT broker settings were correctly configured.
- Icon . This means that the MQTT broker settings were not correctly configured.
- Icon . This means that the MQTT broker cannot connect to the network.

Active	Name	Modified
	silent	01/01/2019 04:01:01
	silent1	22/04/2020 17:09:34

MQTT broker section

This section displays a table containing profiles of the MQTT broker known as Eclipse Mosquitto™, and shows the **Create new** button that lets you create a new profile.

The table displays the following information:

- profile editing access. A predefined profile is read-only. All profiles created by the user can be edited.
- Active** – the active profile is indicated by the .
- Name** – name of the profile. Clicking the icon opens the list of profile settings.
- Modified** – date and time of the most recent change in the profile.

Settings section

In the **Settings** section, you can configure the system settings.

The **Settings** section contains the following blocks of settings:

- [Network](#).
- [System security](#).
- [Web server](#).
- [Utilities](#).
- [General](#).
- [KSC](#).

Network settings block

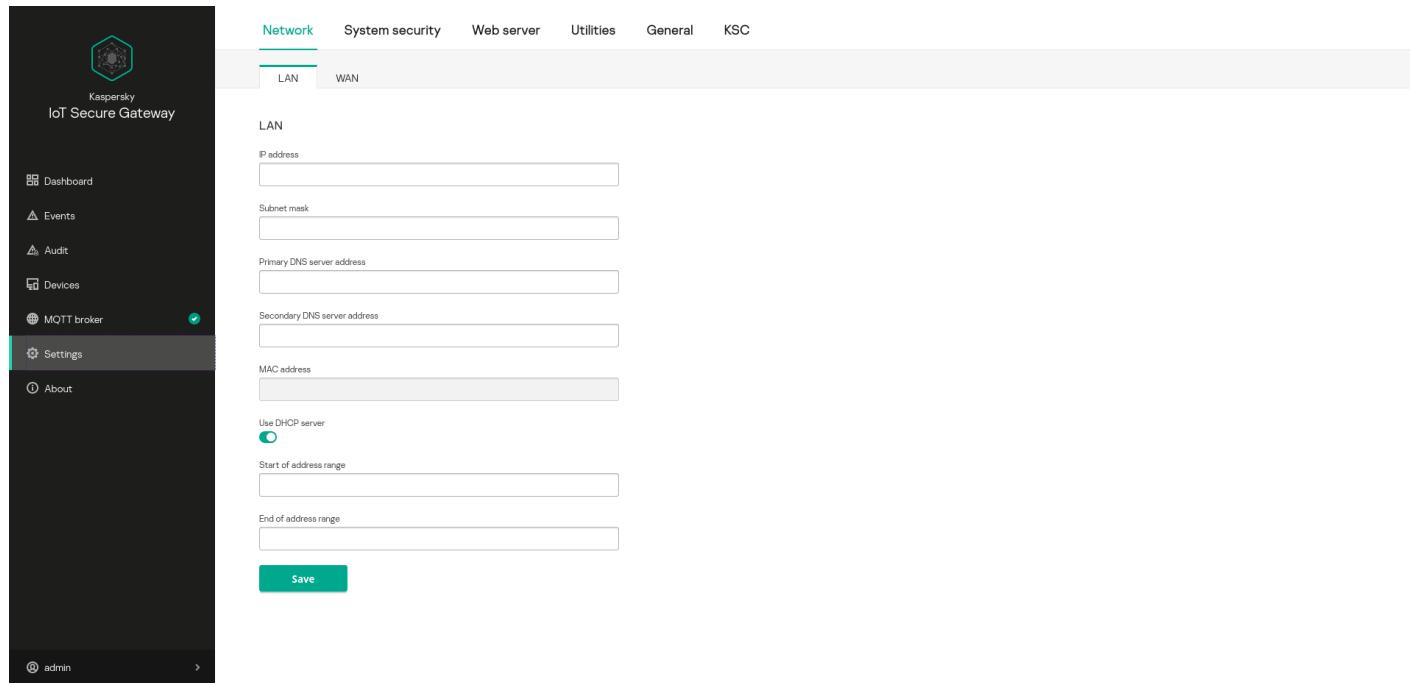
In the **Network** settings block, you can view and change the network settings of Kaspersky IoT Secure Gateway.

The **Network** settings block contains the following tabs:

- **LAN**.
- **WAN**.

LAN tab

On the **LAN** tab (see the figure below), you can view and [change the settings for connecting](#) Kaspersky IoT Secure Gateway to the internal network.



The screenshot shows the Kaspersky IoT Secure Gateway web interface. On the left is a sidebar with icons for Dashboard, Events, Audit, Devices, MQTT broker (with a green checkmark), Settings (selected), and About. The main area has a header with tabs: Network (selected), System security, Web server, Utilities, General, and KSC. Below the tabs is another set of tabs: LAN (selected) and WAN. The LAN tab displays fields for network configuration: IP address, Subnet mask, Primary DNS server address, Secondary DNS server address, MAC address, and a Use DHCP server toggle button. At the bottom are fields for Start of address range and End of address range, and a Save button.

Network settings block. LAN tab

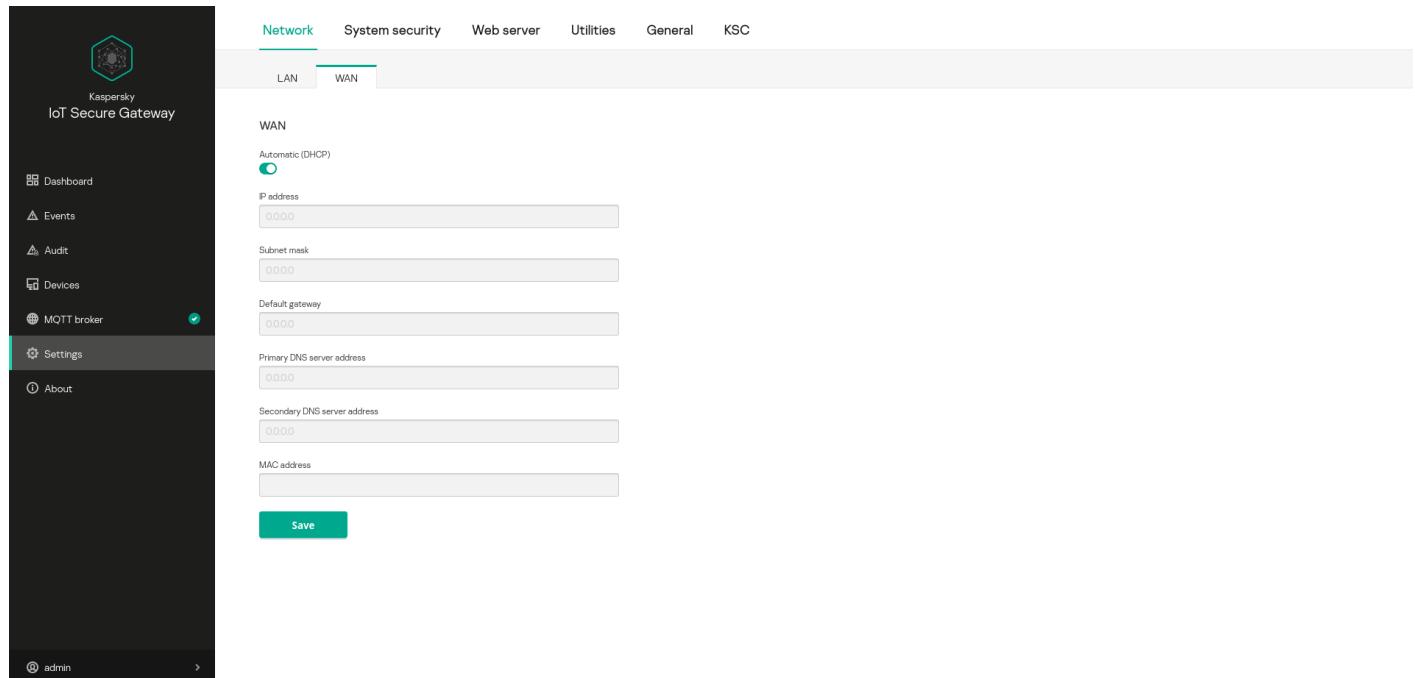
This tab contains the **Use DHCP server** toggle button that lets you automatically configure the network settings, and fields that let you manually configure the internal network settings.

The Kaspersky IoT Secure Gateway internal network can be used to carry out the following tasks:

- Access the Kaspersky IoT Secure Gateway web interface.
- Access the DHCP server.
- Forward event logs to an internal Syslog server.
- Monitor devices that are connected to Kaspersky IoT Secure Gateway.

WAN tab

On the **WAN** tab (see the figure below), you can view and change the settings for connecting Kaspersky IoT Secure Gateway to an external network.



The screenshot shows the Kaspersky IoT Secure Gateway web interface. On the left is a sidebar with icons for Dashboard, Events, Audit, Devices, MQTT broker (with a green checkmark), Settings (which is selected and highlighted in blue), and About. At the bottom of the sidebar are user authentication details (@ admin) and a navigation arrow. The main content area has a header with tabs: Network, System security, Web server, Utilities, General, and KSC. Below the tabs are sub-tabs: LAN and WAN. The WAN tab is selected and highlighted in blue. The main content area is titled 'WAN' and contains the following fields:

- Automatic (DHCP)**: A toggle button that is currently turned on (green).
- IP address**: An input field containing '0.0.0.0'.
- Subnet mask**: An input field containing '0.0.0.0'.
- Default gateway**: An input field containing '0.0.0.0'.
- Primary DNS server address**: An input field containing '0.0.0.0'.
- Secondary DNS server address**: An input field containing '0.0.0.0'.
- MAC address**: An input field containing '00:0C:29:00:00:00'.

 At the bottom of the form is a green 'Save' button.

Network settings block. WAN tab

This tab contains the **Automatic (DHCP)** toggle button that lets you automatically configure the network settings as well as fields [that let you manually configure the external network settings](#).

The Kaspersky IoT Secure Gateway external network can be used to carry out the following tasks:

- Integrate Kaspersky IoT Secure Gateway and Kaspersky Security Center.
- Provide Intrusion Prevention functionality ([IPS component](#)).
- Forward event logs to an external Syslog server.

System security settings block

In the **System security** settings block, you can view and change the security settings of the Kaspersky IoT Secure Gateway system.

In the **Users** block (see the figure below), you can [manage system users](#) and the [password policy](#).

The screenshot shows the 'System security' settings block. The left sidebar includes a logo for 'Kaspersky IoT Secure Gateway' and navigation links for Dashboard, Events, Audit, Devices, MQTT broker (selected), Settings (selected), and About. The user 'admin' is logged in. The top navigation bar has tabs: Network, System security (selected), Web server, Utilities, General, and KSC. The main content area contains two sections: 'Users' (a table with one row for 'admin') and 'Password policy' (a configuration section with various security parameters).

System security settings block

The main part of the **Users** block contains a table of users of the Kaspersky IoT Secure Gateway system. The name of the user account is indicated in the **User name** column.

Under the table is the **Password policy** block, which lets you [configure a password policy](#) for system users.

Web server settings block

In the **Web server** settings block (see the figure below), you can view, [create, delete and change CivetWeb web server profiles](#). This block displays a table containing CivetWeb web server profiles, and a **Create new** button that lets you create a new profile.

The screenshot shows the 'Web server' settings block. The left sidebar includes a logo for 'Kaspersky IoT Secure Gateway' and navigation links for Dashboard, Events, Audit, Devices, MQTT broker (selected), Settings (selected), and About. The user 'admin' is logged in. The top navigation bar has tabs: Network, System security, Web server (selected), Utilities, General, and KSC. The main content area shows a table titled 'Profiles' with one row: 'Default' (Active, Modified: 01/01/2019 04:01:01). A 'Create new' button is located at the bottom of the table.

Web server settings block

The table displays the following information:

- **>Edit** – profile editing access. A predefined profile is read-only. All profiles created by the user can be edited.
- **Active** – the active profile is indicated by the **✓** icon.
- **Name** – name of the profile. Clicking the **+** icon opens the list of profile settings.
- **Modified** – date and time of the most recent change in the profile.

Utilities settings block

In the **Utilities** settings block, you can view and edit the settings for push notifications and for forwarding network security and audit logs to a recipient Syslog server.

The **Utilities** settings block contains the following tabs:

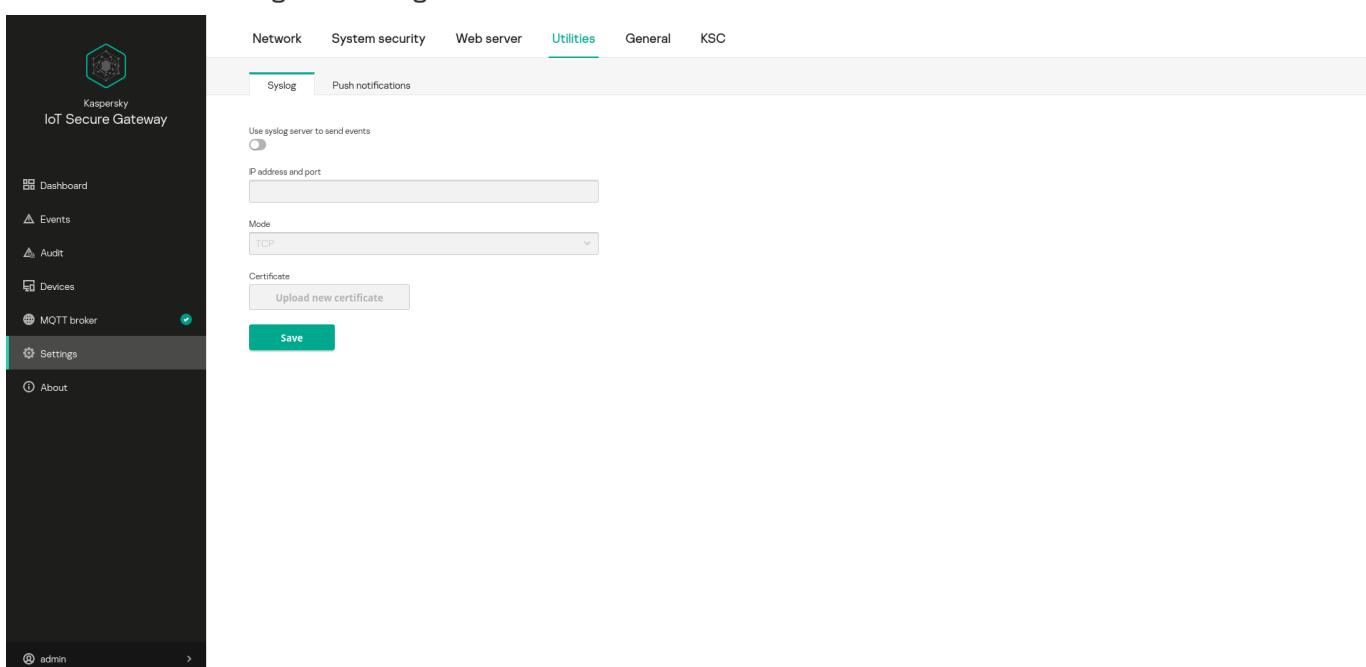
- **Syslog**.
- **Push notifications**.

Syslog tab

On the **Syslog** tab (see the figure below), you can [view and change the settings for forwarding logs](#) containing network security events and system security audit events to a recipient Syslog server.

The main part of the **Syslog** tab displays the following elements:

- **IP address and port** field containing the IP address and port of the Syslog server to which the network security and audit logs are forwarded.
- **Mode** field that lets you select the protocol for forwarding logs.
- **Download new certificate** button for uploading a security certificate to the application.
- **Save** button for saving the settings.

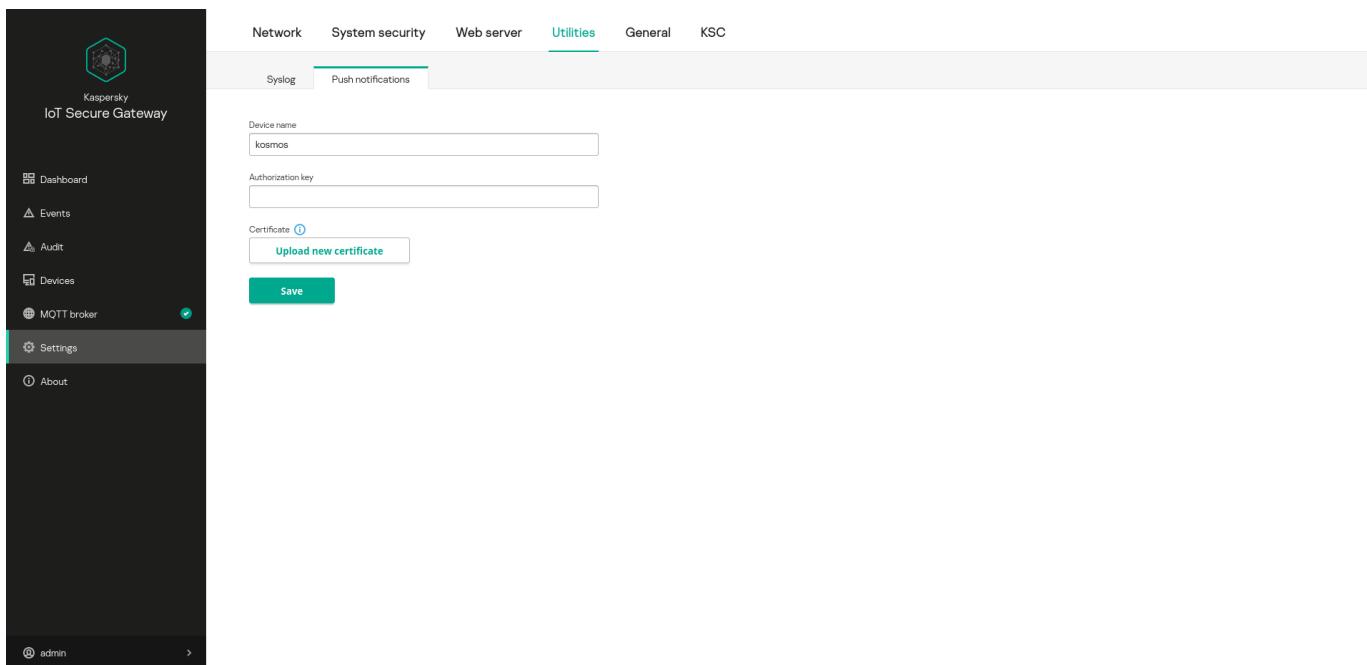


Push notifications tab

On the **Push notifications** tab (see the figure below), you can [configure the settings for forwarding push notifications](#) to a mobile phone.

The main part of the **Push notifications** tab displays the following elements:

- **Device name** field containing the name of the device to which the push notifications are sent.
- **Authorization key** field containing the Firebase authorization key.
- **Download new certificate** button for downloading a certificate.
- ⓘ icon that lets you view information about the uploaded certificate.
- **Save** button for saving the device name.

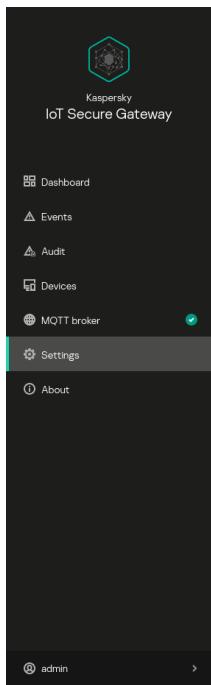


Utilities settings block. Push notifications tab

General settings block

In the **General** settings block, you can view and change the [date and time settings](#) of Kaspersky IoT Secure Gateway.

The **Date and time** block (see the figure below) displays the current date and time values configured in Kaspersky IoT Secure Gateway.



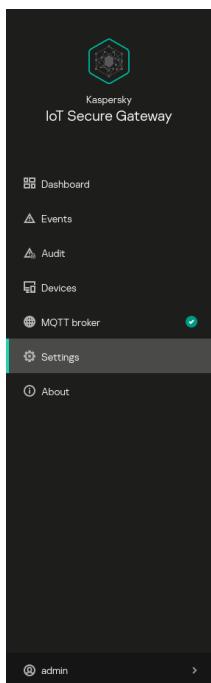
General settings block

The **Change date (UTC)** and **Change time (UTC)** settings blocks contain fields that let you define the current date and time, and a **Save** button that lets you save changes.

Indicate the current time in the UTC time zone.

KSC settings block

In the **KSC** settings block, you can view and edit the Kaspersky Security Center server address.



KSC settings block

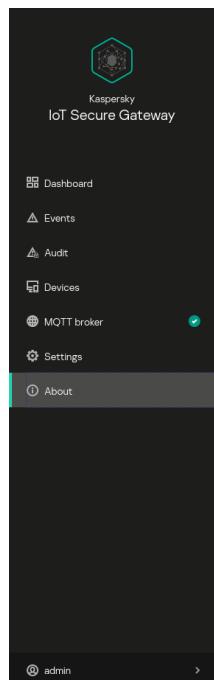
This tab contains fields for specifying the IP address and port of the Kaspersky Security Center server, and a **Save** button that lets you save the changes.

About section

In the **About** section (see the figure below), you can receive concise information about the versions of the Kaspersky IoT Secure Gateway system and the KasperskyOS operating system.

In the **Online Help** block, you can open the online help guide by clicking **Use this link to open online help for Kaspersky IoT Secure Gateway**.

In the **Information about third-party code** block, you can open the file named legal_notices.txt containing information about third-party code by clicking **Use this link to open information about third-party code**.



About section

User menu

The user menu includes the following elements:

- **Change password** – opens a window in which you can [change the password](#) for logging in to Kaspersky IoT Secure Gateway.
- **Language** – lets you switch between Russian and English.
- **Log out** – exit the system.

Data provision

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

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

- User account name.
- IP addresses, MAC addresses, and the names of devices that were detected in the network.
- Event log.
- Audit log.
- User security certificates.
- User settings defined during system configuration.

Each time the system is restarted, the event log and device list are deleted. The next time you log in, the event log and device list begin receiving all new entries. All certificate details are encrypted and stored in a separately allocated space on the drive.

When working with Kaspersky IoT Secure Gateway, cookie files save the session ID, user name, and last visited page of the web interface (if the session was automatically closed after 10 minutes).

If Kaspersky IoT Secure Gateway is connected to the Kaspersky Security Center Web Console, it can save and process the following information that does not include personal data:

- Internal network settings:
 - Status of automatic configuration of internal network settings via the DHCP protocol (enabled or disabled).
 - IP address of Kaspersky IoT Secure Gateway in the internal network.
 - Subnet mask.
 - IP addresses of DNS servers.
 - MAC address of Kaspersky IoT Secure Gateway in the internal network.
 - Starting and ending IP addresses of the range of internal network addresses.
- External network settings:
 - Status of automatic configuration of external network settings via the DHCP protocol (enabled or disabled).
 - IP address of the default gateway.
 - IP address of Kaspersky IoT Secure Gateway in the external network.
 - Subnet mask.
 - MAC address of Kaspersky IoT Secure Gateway in the external network.
 - IP addresses of DNS servers.

- Settings of firewall rules:
 - Status of a rule (enabled or disabled).
 - Action that the firewall must take on 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.
- Information about the Intrusion Prevention system:
 - Status of the Intrusion Prevention system (enabled or disabled).
 - Accessibility of the Intrusion Prevention service.
 - IP addresses in the unauthorized list.
 - IDs of signatures used for adding IP addresses to the unauthorized list.
 - IP addresses on the authorized list.
- MQTT broker profile settings:
 - Indication of whether the profile was predefined.
 - Status of the profile (active or inactive).
 - Profile name.
 - Settings of configuration files and MQTT certificates: file name, type and contents.
- Settings of web server profiles:
 - Indication of whether the profile was predefined.
 - Status of the profile (active or inactive).
 - Profile name.
- Syslog server settings:
 - Indication of whether events are forwarded to a Syslog server.
 - IP address of the Syslog server.
 - Port of the Syslog server.

- Forwarding mode.
- Certificate settings.
- Settings of push notifications:
 - Name of the device to which Kaspersky IoT Secure Gateway sends push notifications.
 - Authentication key.
 - Certificate settings.
- Date and time set in Kaspersky IoT Secure Gateway.
- Password policy.
- Interval for synchronizing settings between the Kaspersky Security Center Web Console and Kaspersky IoT Secure Gateway.
- Commands that the Kaspersky Security Center Web Console can send to Kaspersky IoT Secure Gateway.
- Status of masquerading (enabled or disabled).
- Update server address.
- Product 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.

Licensing Kaspersky IoT Secure Gateway

The terms of use of the application are set forth in the End User License Agreement or in a similar document under which the application is used.

Configuring Kaspersky IoT Secure Gateway

This section describes how to configure Kaspersky IoT Secure Gateway.

Configuring network settings

The Kaspersky IoT Secure Gateway system is delivered with a statically configured IP address. To enable the system to operate as a secure gateway for the Internet of Things, you must configure the settings of the external and internal networks.

An *external network* is a network used by Kaspersky IoT Secure Gateway to access the Internet.

An *internal network* is an enterprise network in which sensors transmit telemetry data to the system.

To configure network settings:

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

The **Network** settings block opens in the **Settings** section.

2. In the **WAN** tab, configure the external network settings:

- If it is necessary to configure network settings automatically based on the DHCP protocol, switch on the **Automatic (DHCP)** toggle button. By default, the **Automatic (DHCP)** toggle button is switched on.
- If you need to configure the network settings manually, switch off the **Automatic (DHCP)** toggle button and specify the following settings:
 - 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 system in the external network.

3. In the **LAN** tab, configure the internal network settings as follows:

- If you need to configure network settings automatically based on the DHCP protocol, switch on the **Use DHCP server** toggle button. By default, the **Use DHCP server** toggle button is switched on.
- If you need to configure the network settings manually, switch off the **Use DHCP server** toggle button and specify the following settings:
 - In the **IP address** field, enter the IP address that you want to assign to the system in the internal network.
 - In the **Subnet mask** field, enter the subnet mask.
 - 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 system in the internal network.
- In the **Address range start** field, enter the starting IP address of the address range.
- In the **Address range end** field, enter the ending IP address of the address range.

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

5. [Reload the Kaspersky IoT Secure Gateway](#) so that the changes to the network settings take effect.

Managing the password policy

Kaspersky IoT Secure Gateway lets you use a password policy to configure the required strength of passwords for system users.

To change the password policy for new system users:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, open the **System security** settings block.
3. In the **Password policy profile** drop-down list in the **Password policy** block, select the relevant policy: *Low security*, *Medium security*, or *High security*. Each policy has predefined password strength requirements indicated under the drop-down list.
4. Click **Save** in the lower part of the page to save the changes.

Changing a user password

To change the password of your user account:

1. In the menu in the left part of the web interface page, select **@<user name>**.
The user menu appears.
2. In the user menu, select **Change password**.
This opens the window for changing the password. To view the current password policy, click the **Current password policy** link.
3. In the **Change password** field, enter the current password of your user account.
4. In the **New password** and **Repeat new password** fields, enter the new password.

You can view the current [password policy](#) by clicking the **Current password policy** link.

5. Click the **Edit** button.

Configuring MQTT broker settings

The MQTT broker Eclipse Mosquitto supports operations of Kaspersky IoT Secure Gateway over the 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 is delivered with a predefined profile that includes an MQTT broker configuration file. Kaspersky IoT Secure Gateway lets you create new profiles, edit existing profiles, and switch between profiles.

Creating a new MQTT broker profile

To create a new MQTT broker profile:

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

You will see a table that lists the MQTT broker profiles.

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

The **Create MQTT profile** pane opens.

3. In the window that opens, in the **Template** drop-down list, select the MQTT broker profile that you want to use to create a new profile (the Eclipse Mosquitto configuration file and security certificates of the selected profile are added to the new profile) or leave it **None** if you want to create an empty profile (you will need to [fill](#) the empty profile).

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.

Completing an empty MQTT broker profile

To complete an empty profile:

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

2. In the **Profiles** table, in the **Name** column, click the icon next to the empty profile (the profile is empty if you created it based on the **None** template and have not yet completed it. A profile is complete if a list of configuration files and certificates is displayed within it).

3. Click the **Download** button in the lower part of the page.

This opens a window for downloading a file to the system.

4. In the opened window, select the certificate file. The file size must not exceed 131 KB.

The certificate file will be downloaded to the system and will appear in the profile.

An Eclipse Mosquitto profile requires multiple security certificates, such as a certificate issued by a Certificate Authority, a server certificate, and a private key file. If your profile prescribes the use of SSL/TLS, repeat this step as many times as required to upload all necessary certificates to the system.

5. Click the **Create new file** button.

The **Create MQTT configuration file** pane opens.

6. In the opened window, in the **Configuration file type** drop-down list, select **Main configuration file**.

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

8. Click **Save** to save the Eclipse Mosquitto configuration file.

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

9. In the profile table, click the name of the configuration file that was just created.

The configuration file properties window opens.

10. In the lower part of the opened window, click the  icon.

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

11. Type the required Eclipse Mosquitto settings in the text editor window.

For more details on the parameters of the Eclipse Mosquitto configuration file, please refer to the documentation on the [developer's website](#). Please note that there are [limitations](#) when configuring the MQTT broker Eclipse Mosquitto for Kaspersky IoT Secure Gateway.

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

Modifying an MQTT broker profile

To modify an MQTT broker profile:

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

2. In the **Profiles** table, in the **Name** column, click the  icon next to the profile that you want to change.

If the profile was created based on a different profile, you will see a list of configuration files and certificates that are included in the profile. If an empty profile was created, the list of files will be empty and you need to [complete](#) the profile.

3. Click the name of the profile's configuration file.

The **Edit MQTT configuration file** window opens.

4. In the lower part of the opened window, click the  icon.

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

For more details on the parameters of the Eclipse Mosquitto configuration file, please refer to the documentation on the [developer's website](#). Please note that there are [limitations](#) when configuring the MQTT broker Eclipse Mosquitto for Kaspersky IoT Secure Gateway.

5. In the text editor window, change the MQTT broker settings as required.

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

The text editor window closes.

7. If you need to add a security certificate to the profile, click the **Download** button in the lower part of the page.

This opens a window for downloading a file to the system.

8. In the opened window, select the certificate file.

The certificate file will be downloaded to the system and will appear in the profile.

9. If you need to remove a security certificate from the profile, click the name of this certificate in the **Profiles** table.

The certificate properties window opens.

10. Click the  icon.

11. In the window that opens, confirm deletion of the certificate.

Switching to a different MQTT broker profile

To switch to another MQTT broker profile:

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

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

The **Edit MQTT profile** window opens.

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

In the **Profiles** table, in the **Active** column, the  icon appears next to the active profile.

Limitations when configuring an MQTT broker

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

- In the `include_dir` parameter, you can specify only one folder containing configuration files.
- You cannot specify file paths using the `capath` and `bridge_capath` parameters.
- The `log_dest stdout` parameter prints the MQTT log by using the Kaspersky IoT Secure Gateway API.
- The `bridge_require_ocsp` parameter is not supported.
- The `persistence` and `websockets` settings are not supported.
- The client ID (`clientid`) must be explicitly defined (for example, via `use_username_as_clientid`).
- The `auth_plugin` parameter is not supported.
- Arguments of the `ciphers` parameter are defined in mbedTLS format instead of openssl.

- The `log_dest file`, `pid_file` and `http_dir` parameters are not supported.

Configuring the web server

Operation of the Kaspersky IoT Secure Gateway web interface is supported by a CivetWeb web server. Web server settings are stored in a web server profile. A web server profile binds a CivetWeb configuration file to a security certificate. Kaspersky IoT Secure Gateway is delivered with a predefined profile that includes a security certificate signed by Kaspersky.

After the system is turned on for the first time, you must replace the security certificate installed by default for the [web server](#) with the security certificate that is used in your organization.

Kaspersky IoT Secure Gateway lets you create new profiles, edit existing profiles, and switch between profiles. Different profiles enable you to work with different security certificates.

Creating a new web server profile

To create a new web server profile:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, select the **Web server** tab.
You will see a table that lists the web server profiles.
3. Click the **Create new** button in the lower part of the page.
The **Create web server profile** pane opens.
4. In the opened pane, in the **Template** drop-down list, select the web server profile that you want to use to create a new profile (the CivetWeb configuration file and security certificate of the selected profile are added to the new profile) or leave **None** if you want to create an empty profile (you will need to [fill](#) the empty profile).
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.

Completing an empty web server profile

To complete an empty profile:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, select the **Web server** tab.
3. In the **Profiles** table, in the **Name** column, click the  icon next to the empty profile (the profile is empty if you created it based on the **None** template and have not yet completed it. A profile is complete if a configuration file is displayed within it).

4. Click the **Download** button in the lower part of the page.

This opens a window for downloading a file to the system.

5. In the opened window, select the certificate file in the PEM format. The file size must not exceed 131 KB.

The certificate file will be downloaded to the system and will appear in the profile.

6. Click the **Create new file** button.

The **Create web server configuration file** pane opens.

7. In the window that opens, in the **Name** field, enter the name of the new configuration file using letters of the English alphabet.

8. Click **Save** to save the CivetWeb configuration file.

The **Create web server configuration file** pane closes.

9. In the profile table, click the name of the configuration file that was just created.

The **Edit web server configuration file** pane opens.

10. In the lower part of the pane, click the  icon.

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

11. Type the following CivetWeb settings in the text editor window: `ssl_certificate <certificate name>`, where `<certificate name>` is the name of the certificate file that was loaded at step 5.

The current version of Kaspersky IoT Secure Gateway supports only one CivetWeb setting: `ssl_certificate`.

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

Modifying the web server profile

To modify a web server profile:

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

2. In the **Settings** section, open the **Web server** settings block.

3. In the **Profiles** table, in the **Name** column, click the  icon next to the profile that you want to change.

If the profile was created based on a different profile, you will see a list of files that are included in the profile. If an empty profile was created, the list of files will be empty and you need to [complete](#) the profile.

4. Click the name of the profile's configuration file.

The **Edit web server configuration file** pane opens.

5. In the lower part of the opened window, click the  icon.

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

6. In the text editor window, change the web server settings as required.

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

The text editor window closes.

8. If you need to add a security certificate to the profile, click the **Download** button in the lower part of the page.

This opens a window for downloading a file to the system.

9. In the opened window, select the certificate file.

The certificate file will be downloaded to the system and will appear in the profile.

10. If you need to remove a security certificate from the profile, click the name of this certificate in the **Profiles** table.

The certificate properties window opens.

11. Click the  icon.

12. In the window that opens, confirm deletion of the certificate.

Switching to a different web server profile

To switch to another web server profile:

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

2. In the **Settings** section, select the **Web server** tab.

3. In the **Profiles** table, in the **Name** column, click the name of the profile that you want to set as active.

The **Edit web server profile** window opens.

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

In the **Profiles** table, in the **Active** column, the  icon appears next to the active profile.

Configuring the date and time

To configure date and time settings:

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

The **Network** settings block opens in the **Settings** section.

2. In the **Settings** section, open the **General** settings block.

3. Configure the date settings. To do so, in the **Date** block, use the **Day**, **Month** and **Year** drop-down lists to specify the current date.

4. Click the **Save** button in the **Date** block to save the changes.

5. Configure the time settings. To do so, in the **Time** block, use the **Hours**, **Minutes**, and **Seconds** drop-down lists to specify the current time.

6. Click the **Save** button in the **Time** block to save the changes.

Indicate the current time in the UTC time zone.

Monitoring devices

The **Devices** section displays information about devices that the system detected in the network.

The system divides detected devices into trusted devices and untrusted devices. Each new device detected by the system in the network is considered to be an untrusted device. To make a device trusted, you need to add it to the authorized list.

When an untrusted device appears in the network, contact the employee responsible for data security in your organization.

Information about detected devices is consolidated into a table containing the following columns:

- **Name** – name of the device.
- **Type** – type of device.
- **Status** – status of the device (*Unauthorized* or *Authorized*).
- **MAC address** – MAC address of the device.
- **IP address** – IP address of the device.
- **Details** – operating system and vendor of the device (if identified).

If necessary, you can sort the device table based on any column by clicking the column header.

The table displays the devices detected by the system when the **Devices** section is opened. The device table is not updated automatically.

To update the list of detected devices:

In the **Devices** section, click the **Update** button in the upper part of the page.

By default, the **Devices** table displays all unauthorized devices of all detected types, and all buttons in the **Type** block are highlighted in blue. If the **Whitelist** toggle button is switched on, all authorized devices are displayed.

To filter the list of displayed devices by device type:

In the **Devices** section, click the button containing the name of the device type in the **Type** block located above the table.

Devices of the selected type will disappear from the **Devices** table, and the button with the device type will no longer be highlighted. If you need the table to display devices that were filtered out of the display, you need to click the button with the name of this device type again (the button will be highlighted in blue).

Working with the list of authorized devices

An authorized list contains authorized devices.

To show only the devices that are included in the authorized list:

1. In the menu in the left part of the web interface page, select the **Devices** section.
2. In the **Devices** section, switch on the **Whitelist** toggle button in the upper part of the page.

To show all unauthorized devices:

In the **Devices** section, switch off the **Whitelist** toggle button in the upper part of the page.

To add a device to the authorized list:

1. In the menu in the left part of the web interface page, select the **Devices** section.
2. Select the check box next to the name of the unauthorized device that you want to add to the authorized list.
A pane containing the device icon will open in the right part of the page.
3. In the opened pane, click the **Add to whitelist** button.

The pane containing the device icon closes. The device will appear in the authorized list.

To remove a device from the authorized list:

1. In the menu in the left part of the web interface page, select the **Devices** section.
2. Select the check box next to the name of the trusted device that you want to remove from the authorized list.
A pane containing the device icon will open in the right part of the page.
3. In the opened pane, click the **Remove from whitelist** button.

The pane containing the device icon closes. The device will be removed from the authorized list.

Monitoring events

Kaspersky IoT Secure Gateway maintains two types of event logs:

- A *network security log* saves events related to network security, such as the detection of new devices in the network.
- An *audit log* saves events associated with the security of Kaspersky IoT Secure Gateway, such as the security status of components after the application is loaded.

Kaspersky IoT Secure Gateway lets you view [network security](#) and [audit](#) logs through the web interface, and forward them to a [recipient Syslog server](#).

Kaspersky IoT Secure Gateway lets you use [push](#) technology and the [MQTT](#) protocol to send notifications about events that occur.

Viewing the network security log

Kaspersky IoT Secure Gateway lets you view network security events that occur during the current session of the user's connection to the system through a browser. These events are created by [system components](#). In the **Entity** column, the name of the source component is indicated for each event (for example, the *Auth server. LoginError. Bad login or password event is sent by the Auth server* component and indicates that there was an attempt to log in to the system with an incorrect user account name or password).

To view network security events:

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

You will see a table containing network security events.

*To sort events in the table of the **Network security events** section:*

- To sort by the name of the entity that registered the event, click the header of the **Entity** column.
- To sort by event type, click the header of the **Event** column.
- To sort by event text, click the header of the **Title** column.
- To sort by date and time, click the header of the **Date and time** column.

Viewing the audit log

Kaspersky IoT Secure Gateway saves events related to system security in the audit log. These events are created by [system components](#). Each event indicates the name of the source component.

When an event with critical severity occurs, contact the employee responsible for data security in your organization.

To view the audit log:

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

This opens the **System security audit** section that displays a table containing system security events.

*To sort events in the table of the **System security audit** section:*

- To sort by event severity, click the header of the **Severity** column.
- To sort by event text, click the header of the **Title** column.
- To sort by the name of the entity that registered the event, click the header of the **Entity** column.
- To sort by date and time, click the header of the **Date and time** column.

To save the audit log to your computer:

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

2. In the **System security audit** section, click the **Download All** button.

This opens a window warning you that the audit log will be deleted from Kaspersky IoT Secure Gateway after you save the file.

3. Confirm deletion of the audit log from the system.

You will see a window that lets you save the audit log to a file.

4. In the window that opens, specify the path for saving the audit log file.

By default, the audit file is saved with the name audit.csv.

5. Save the file.

To view information about the audit settings:

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

2. Move your mouse cursor over the  icon in the upper part of the window.

This opens a pop-up window containing the following information:

- **Total** – current number of entries in the audit log.
- **Capacity** – maximum number of entries in the audit log.
- **Policy** – audit log maintenance policy.
 - *Circular* – when the audit log is overfilled, new entries will overwrite old entries.
 - *Limited* – when the audit log is overfilled, the system stops.

Forwarding event logs to a Syslog server

Kaspersky IoT Secure Gateway can send network security event and audit logs to a Syslog server.

To configure forwarding of event logs to a Syslog server:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, open the **Utilities** settings block.
The **Syslog** tab opens in the **Utilities** settings block.
3. To enable forwarding of event logs to a Syslog server, switch on the **Use syslog server to send events** toggle button.
4. Configure the settings for forwarding network security event and audit logs to a recipient Syslog server. To do so, specify the following settings on the **Syslog** tab:
 - In the **IP address and port** field, enter the IP address and port of the recipient Syslog server, separating them with a colon like in the following example: 198.51.100.0:514.
 - In the **Mode** drop-down list, select the protocol that will be used by Kaspersky IoT Secure Gateway to send network security event and audit logs to the recipient 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 **Download new certificate** button and select the relevant security certificate in the opened window.
5. Click **Save** in the lower part of the page to save the changes.

Forwarding push notifications

Kaspersky IoT Secure Gateway uses [Firebase™ Cloud Messaging \(FCM\)](#) to forward push notifications about events in the form of JSON messages over the HTTPS protocol to the address <https://fcm.googleapis.com/fcm/send>. The system relays information about its name and provided topics of push notifications every 4 seconds to the topic /topics/DevicesandTopics residing in the FCM cloud service.

Example of JSON data sent by the system indicating its name and provided topics of push notifications:

```
{  
  "data": {  
    "Device" : "Device-1",  
    "Audit" : "NewRecord",  
    "TrafficProcessor" : "NewDevice, DeviceUpdate",  
  },  
  "to": "/topics/DevicesAndTopics"  
}
```

In this case, the system named Device-1 lets you subscribe to push notifications about NewRecord, NewDevice and DeviceUpdate events.

A push notification about an event is sent to the topic /topics/DeviceName_EntityName_EventType, where:

- DeviceName is the name of the device.
- EntityName is the name of the entity that registered the event.
- EventType is the type of event.

Example of JSON data sent by the system regarding an event that occurred:

```
{
  "data": {
    "data" : "Some data about new device",
  },
  "to": "/topics/Device-1_TrafficProcessor_NewDevice"
}
```

To receive push notifications, you can create your own application that works with FCM. To do so, you will need a google-services.json configuration file and the system name.

To configure the system name for sending push notifications:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, open the **Utilities** tab.
3. Select the **Push notifications** tab.
4. In the **Device name** field, enter the name that will be used by the system to send push notifications.
5. In the **Authorization key** field, enter the Firebase authorization key.
6. Click **Save** in the lower part of the page to save the changes.

For more detailed information about creating an application to receive push notifications, please refer to the [Firebase Cloud Messaging documentation](#).

Forwarding MQTT notifications

Kaspersky IoT Secure Gateway can send notifications about security events and 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 the **MQTT broker** section.
2. In the **Profiles** table, in the **Name** column, click the icon next to the active profile.
3. Select the profile's configuration file.

The **Edit MQTT configuration file** window opens.

4. In the lower part of the opened window, click the icon.

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

5. In the text editor window, add the MQTT broker settings to the beginning of the file.

The system supports the following additional settings for configuring MQTT notifications:

- `kos_audit <value>`. If the value is set to `true`, Kaspersky IoT Secure Gateway sends audit events over the MQTT protocol. If the value is set to `false`, Kaspersky IoT Secure Gateway does not send audit events over the MQTT protocol. By default, the value is set to `true`.
- `kos_event <value>`. If the value is set to `true`, Kaspersky IoT Secure Gateway sends security events over the MQTT protocol. If the value is set to `false`, Kaspersky IoT Secure Gateway does not send security events over the MQTT protocol. By default, the value is set to `false`.
- `kos_audit_topic <Topic name>`. This lets you define the topic for sending audit events. This setting is ignored if `kos_audit` is set to `false`. By default, the topic name is set to `SGW/audit`.
- `kos_event_topic <Topic name>`. This lets you define the topic for sending audit events. This setting is ignored if `kos_event` is set to `false`. By default, the topic name is set to `SGW/event`.

6. If you are using a network bridge, configure topic mapping in the Connection section of the configuration file. For more details on the parameters of the Eclipse Mosquitto configuration file, please refer to the documentation on the [developer's website](#).

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

The text editor window closes.

Intrusion Detection

Kaspersky IoT Secure Gateway lets you use Intrusion Detection rules to detect intrusions from an external network into the internal enterprise network.

An *Intrusion Detection rule* describes a traffic anomaly that could be a sign of an attack from an external network. Rules contain the conditions that the Intrusion Detection system uses to analyze traffic. Intrusion Detection rules are stored in Kaspersky IoT Secure Gateway.

Intrusion Detection rules are provided by Kaspersky and are intended for detecting signs of the most frequently encountered attacks or suspicious network activity. Intrusion Detection rules are available immediately after Kaspersky IoT Secure Gateway is installed. You can update Intrusion Detection rules by [installing updates](#).

Additionally, you can enable the Kaspersky IoT Secure Gateway Intrusion Prevention System (which is disabled by default). The Intrusion Prevention System allows you [to add device IP addresses to the authorized and unauthorized list](#). You can add the IP addresses of devices with traffic found to contain suspicious activity to the list of unauthorized devices. If the Intrusion Prevention System is switched off, security events will be written to the security log.

You can view the list of detected and blocked intrusions in the [network security log](#). You can manage [IPS component](#) settings [through the web plug-in of the Kaspersky Security Center Web Console](#).

Monitoring the state of Kaspersky IoT Secure Gateway

You can track the state of the Kaspersky IoT Secure Gateway system through the web interface. This section contains instructions on monitoring the state of Kaspersky IoT Secure Gateway.

Viewing information about system users

The current version of Kaspersky IoT Secure Gateway has only one user, the system administrator.

To view information about system users:

1. In the menu in the left part of the web interface page, select the **Settings** section.
2. In the **Settings** section, select the **System security** tab.

All system users are listed on the **System security** tab in the table in the **Users** block.

Viewing the state of components

Kaspersky IoT Secure Gateway lets you track the security state of [system components](#).

To view the security state of system components:

1. In the menu in the left part of the web interface page, select the **Dashboard** section.
2. Click the **Show** link in the **Security state** block to open the list of system components.

The list of system components will be displayed. The security state of each component is shown on the left of the component name (see the figure below). To close the list of system components, click the **Hide** link.

Security state	
Tee manager	
Logger	
Deployer	
Ids	
Config manager	
Secure storage	
Secure manager	
Traffic processor	
Auth server	
Traffic controller	

Security state of system components

If a red icon is displayed near the name of any component, contact the employee responsible for data security in your organization.

Managing the application through the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console lets you remotely manage the operation of Kaspersky IoT Secure Gateway. You can use the capabilities of the Kaspersky Security Center Web Console to do the following:

- Configure MQTT broker settings.
- Configure network settings.
- Manage the firewall.
- Manage the Intrusion Detection system.
- Configure web server settings.
- Configure forwarding of messages to a Syslog server.
- Configure forwarding of push notifications.
- Configure the date and time.
- Manage the password policy.
- Configure the settings for interaction with the Kaspersky Security Center Web Console.
- Restart and update Kaspersky IoT Secure Gateway.

About the Kaspersky IoT Secure Gateway administration web plug-in

The Kaspersky IoT Secure Gateway administration web plug-in (hereinafter also referred to as simply the "web plug-in") facilitates interaction between Kaspersky IoT Secure Gateway and Kaspersky Security Center.

The web plug-in lets you centrally perform the following operations:

- Manage the settings of Kaspersky IoT Secure Gateway.
- Receive events from Kaspersky IoT Secure Gateway.

To enable interaction between Kaspersky IoT Secure Gateway and Kaspersky Security Center, the following conditions must be fulfilled:

- Kaspersky Security Center settings were specified during configuration of Kaspersky IoT Secure Gateway.
- The Kaspersky IoT Secure Gateway management plug-in was installed in the Kaspersky Security Center Web Console.

Installing the Kaspersky IoT Secure Gateway administration web plug-in

The web plug-in is not installed in the Kaspersky Security Center Web Console by default. You must install the web plug-in on the computer that has the Kaspersky Security Center Web Console installed. The web plug-in functionality is available to all administrators that can access the Kaspersky Security Center Web Console in a browser. You can view the list of installed web plug-ins in the Kaspersky Security Center Web Console interface (**Console settings → Plug-ins**).

To install the web plug-in in the Kaspersky Security Center Web Console:

Find the ZIP archive containing the web plug-in distribution package that you received in the distribution kit and add it to the Kaspersky Security Center Web Console. For more details about adding a distribution package to the Kaspersky Security Center Web Console, please refer to the *Online Help for Kaspersky Security Center*.

Please note that the "mobile protocol" is utilized for interaction between Kaspersky IoT Secure Gateway and Kaspersky Security Center. Make sure that port 13292 (required for connecting mobile devices) is accessible on the Administration Server on which Kaspersky Security Center is installed. For more details about managing mobile devices, please refer to the section titled "Scenario: Mobile Device Management deployment" in the *Online Help for Kaspersky Security Center 12*.

Logging into and logging out of the Kaspersky Security Center Web Console

To log in to the Kaspersky Security Center Web Console, you need to ask the administrator for the web address of the Administration Server and the port number that was specified during installation (port 8080 is used by default). You must also enable JavaScript in your web browser.

To log in to the Kaspersky Security Center Web Console:

1. In your browser, go to <Administration Server web address>:<Port number>.

The login page opens.

2. Log in using the user name and password of a local administrator.

If the Administration Server does not respond or you entered incorrect account credentials, an error message will be displayed.

After logging in, you will see the Dashboard displaying the last language and theme that were used.

If you are logging in to the Kaspersky Security Center Web Console for the first time, a tutorial is displayed in the lower part of the screen. You may follow the instructions of the tutorial, or close it by clicking the close button (X).

You can navigate through the pages of the Kaspersky Security Center Web Console and work with it as required. For additional information about how the Kaspersky Security Center Web Console works, please refer to the *Online Help for Kaspersky Security Center*.

To log out of the Kaspersky Security Center Web Console:

1. In the upper-right corner of the screen, click on your user name.
2. In the drop-down menu, select **Log out**.

The Kaspersky Security Center Web Console closes and the login page is displayed.

Configuring how events are displayed in the Kaspersky Security Center Web Console

For the Kaspersky Security Center Web Console to display events that occur on the device where Kaspersky IoT Secure Gateway is installed, you need to move this device to the managed devices group and create a policy for this device.

To configure the display of events in the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices → Policies and policy profiles**.
2. Click the **Add** button.
The New Policy Wizard starts.
3. In the **Application name** list, select Kaspersky IoT Secure Gateway and click **Next**.
4. Click the **Save** button.
5. In the main window of the Kaspersky Security Center Web Console, select **Device discovery and deployment → Unassigned devices**.
6. Select the check box next to the device name.
7. Click the **Move to group** button.
The **Move to group** pane opens.
8. Select the check box next to the **Managed devices** administration group.
9. Click the **Move** button.

The device will be moved to the managed devices group, and you will be able to view events that occur on this device.

To view events that occurred on a device:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices → Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running.
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Click the **Events** tab.

Configuring Kaspersky IoT Secure Gateway settings through the Kaspersky Security Center Web Console

You can configure the Kaspersky IoT Secure Gateway settings through the web plug-in for the Kaspersky Security Center Web Console.

Configuring MQTT broker settings through the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console lets you create new [MQTT broker profiles](#), edit existing profiles, and switch between profiles.

Creating a new MQTT broker profile through the Kaspersky Security Center Web Console

To create a new MQTT broker profile through the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **MQTT** section.

7. Click the **Add** button above the list of MQTT broker profiles.

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, configurations from the profile are uploaded to the MQTT broker and access to certificates from the profile is activated for the broker. Only one profile can be active.
- **Inactive**, if you do not want to make a new profile active.

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

10. If you want to add a configuration file or certificate to the new profile:

a. In the **List of files** area, click the **Add** button.

The file upload pane opens.

b. In the **Type** drop-down list, select the type of file that you want to add.

c. Click the **Download file** button.

This opens a window for downloading a file to the system.

d. In the opened window, select the configuration file or certificate. The file size must not exceed 131 KB.

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

e. Click **OK** in the lower part of the pane.

The file upload pane closes.

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.

Editing an MQTT broker profile through the Kaspersky Security Center Web Console

To edit an MQTT broker profile through the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.

2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **MQTT** section.

7. In the list of MQTT broker profiles, select the profile that you want to edit.

8. Click the **Edit** button above the list of MQTT broker profiles.

The **Edit profile** window opens.

9. Change the profile settings as necessary:

- To change the settings of the active profile:

- a. In the **Status** drop-down list, select **Inactive**.
 - b. Click **OK** in the lower part of the **Edit profile** window.
The **Edit profile** window closes.
- c. Repeat the steps of these instructions again, starting with step 7.
- In an inactive profile, you can change any settings.

10. Click **OK** in the lower part of the **Edit profile** window.

The **Edit profile** window closes.

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

Deleting an MQTT broker profile through the Kaspersky Security Center Web Console

If you delete all profiles, the MQTT broker functionality will be disabled but Kaspersky IoT Secure Gateway will continue to work.

To delete an MQTT broker profile through the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **MQTT** section.
7. In the list of MQTT broker profiles, select the profile that you want to delete.
8. Click the **Delete** button above the list of MQTT broker profiles.
9. Click **Save** in the lower part of the window to save the changes.

Configuring network settings through the Kaspersky Security Center Web Console

The Kaspersky IoT Secure Gateway system is delivered with a statically configured IP address for the internal interface. To enable the system to operate as a secure gateway for the Internet of Things, you must configure the settings of the external and internal networks.

You can [configure a network by using the web interface](#) of Kaspersky IoT Secure Gateway or through the Kaspersky Security Center Web Console.

To configure network settings through the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Network** section.
7. In the **Network** section, select the **LAN** tab.
8. Configure the internal network settings.
 - If you want to configure internal network settings automatically using the DHCP protocol, switch on the **Automatic (DHCP)** toggle button.
 - If you want to manually configure the internal network settings:
 - In the **IP address** field, enter the IP address that you want to assign to the system in the internal network.
 - In the **Subnet mask** field, enter the subnet mask.
 - In the **Primary DNS server** field, enter the IP address of the primary DNS server.
 - In the **Secondary DNS server** field, enter the IP address of the secondary DNS server.
 - The **MAC address** field displays the MAC address of the system in the internal network.
 - In the **Address range start** field, enter the starting IP address of the address range.
 - In the **Address range end** field, enter the ending IP address of the address range.
9. Click the **Save** button.
10. In the **Network** section, select the **WAN** tab.
11. Configure the external network settings:
 - If you want to configure external network settings automatically using the DHCP protocol, switch on the **Automatic (DHCP)** toggle button.

- If you want to manually configure the external network settings:
 - 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 **Network gateway** field, enter the IP address of the network gateway.
 - In the **Primary DNS server** field, enter the IP address of the primary DNS server.
 - In the **Secondary DNS server** field, enter the IP address of the secondary DNS server.
 - The **MAC address** field displays the MAC address of the system in the external network.

12. Click the **Save** button.

Managing the firewall

You can use the firewall that is built in to Kaspersky IoT Secure Gateway to control and filter traffic transversing the device. [Network traffic is processed](#) according to [firewall rules](#) that are defined through the Kaspersky Security Center Web Console. Traffic that is not explicitly allowed by firewall rules is blocked.

About firewall rules

Firewall rules are divided into *preset firewall rules* and *custom firewall rules*.

Preset firewall rules are used to ensure full-fledged operation of Kaspersky IoT Secure Gateway. You cannot edit these rules, and they are not displayed in the Kaspersky IoT Secure Gateway web plug-in.

If necessary, you can [create](#) additional rules. These rules are called custom firewall rules. You can also [change](#) or [delete](#) rules of this type. Custom firewall rules are checked in the order defined in the Kaspersky Security Center Web Console, from top to bottom. You can create up to 1,000 custom firewall rules.

Kaspersky IoT Secure Gateway supports rules for the following protocols:

- TCP.
- UDP (only IPv4)

SPI (*Stateful Packet Inspection*) is switched on for all of these protocols.

Preset rules allow the following Kaspersky IoT Secure Gateway connections:

- Outgoing connections to the Kaspersky Security Center Web Console server over the TCP protocol
- Outgoing connections to the update server over the TCP, UDP, and TCP/TLS protocols
- Incoming connections to the local web server over the HTTPS protocol
- Outgoing connection to the Syslog server over the TCP, 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

Creating firewall rules

To create a new firewall rule:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
3. The computer properties window opens.
4. Select the **Applications** tab.
5. Click on Kaspersky IoT Secure Gateway.
6. This opens a window containing information about Kaspersky IoT Secure Gateway.
7. Select the **Application settings** tab.
8. Select the **Network** section.
9. Select the **Firewall** tab.
10. Click the **Add** button above the list of firewall rules.

This opens the pane for adding a firewall rule.

11. Specify the settings of the new rule:

- In the **Status** drop-down list, select whether the rule should be enabled:
 - **Enabled.**
The rule is enabled.
 - **Disabled.**
The rule is disabled.
- In the **Action** drop-down list, select the action that the firewall must take on traffic that matches the rule:
 - **Accept.**
Allow the traffic to pass through.
 - **Deny.**
Block traffic from passing through.
- In the **Zone** drop-down list, select the zone to which the rule should be applied:
 - **LAN.**

The rule is applied to traffic that passes from the internal network to an external network.

- **WAN.**

The rule is applied to traffic that passes from an external network to the internal network.

- In the **IP address (source)** field, specify the IP address of the traffic source.
- In the **Port (source)** field, specify the port of the traffic source if this parameter is applicable to the protocol.
- In the **IP address (target)** field, specify the IP address of the traffic destination.
- In the **Port (target)** field, specify the port of the traffic destination if this parameter is applicable to the protocol.
- In the **Protocol** drop-down list, select the utilized protocol.

12. Click the **Save** button.

Custom firewall rules are checked in the order defined in the Kaspersky Security Center Web Console, from top to bottom until the first match. To learn how to change the order of custom firewall rules, please refer to the section titled "[Changing the order of firewall rules](#)".

Editing firewall rules

To edit a firewall rule:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
5. This opens a window containing information about Kaspersky IoT Secure Gateway.
6. Select the **Application settings** tab.
7. Select the **Network** section.
8. Select the **Firewall** tab.
9. Select the check box next to the rule that you want to edit.
10. Click the **Edit** button above the list of firewall rules.
This opens the pane for editing a firewall rule.

11. Change the rule settings as necessary.

12. Click the **Save** button.

Changing the order of firewall rules

To move a firewall rule up or down:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
5. This opens a window containing information about Kaspersky IoT Secure Gateway.
6. Select the **Application settings** tab.
7. Select the **Network** section.
8. Select the **Firewall** tab.
9. Select the check box next to the rule that you want to move up or down.
10. Do one of the following:
 - If you want to move the firewall rule up, click the **Up** button.
 - If you want to move the firewall rule down, click the **Down** button.
11. Click the **Save** button.

Deleting firewall rules

To delete a firewall rule:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.
5. This opens a window containing information about Kaspersky IoT Secure Gateway.
6. Select the **Application settings** tab.
7. Select the **Network** section.
8. Select the **Firewall** tab.
9. Select the rule that you want to delete.
10. Click the **Delete** button above the list of firewall rules.
The rule will be deleted.
11. Click the **Save** button.

Managing the Intrusion Prevention system

Kaspersky IoT Secure Gateway can use the built-in Intrusion Prevention System to analyze and filter traffic. For Intrusion Detection purposes, Kaspersky IoT Secure Gateway uses a signature database that is updated when the device firmware is flashed. When a match is found with a signature from the database, Kaspersky IoT Secure Gateway automatically blocks traffic from the IP address from which the attack originated.

The Intrusion Prevention system is disabled by default.

To enable the Intrusion Prevention System:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Network** section.
7. Select the **IPS** tab.
8. Flip the toggle switch in the upper part of the window to **Intrusion Prevention System is on**.
9. Click the **Save** button.

To enable the denylist:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.

2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Network** section.

7. Select the **IPS** tab.

8. Click the **Show list** button next to the **Blacklist** heading.

The **Blacklist** page opens.

9. Set the toggle button to **Blacklist is enabled**.

10. Click the **Save** button.

To add an IP address to the authorized list:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.

2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Network** section.

7. Select the **IPS** tab.

8. Click the **Show list** button next to the **Whitelist** heading.

The **Whitelist** page opens.

9. Click the **Add** button.

The **Edit** page opens.

10. In the **IP address (source)** field, specify the IP address from which you want to allow traffic.

11. Click the **Save** button.

Procedure for processing network traffic

Kaspersky IoT Secure Gateway handles network traffic according to [firewall rules](#) and authorized and unauthorized lists, which are defined by the [Intrusion Prevention System](#).

Kaspersky IoT Secure Gateway applies rules in the following order:

1. Preset firewall allow rules.

2. Authorized list.

3. Unauthorized list.

4. Custom firewall rules.

5. Preset firewall block rules.

Managing the web server through the Kaspersky Security Center Web Console

Operation of the Kaspersky IoT Secure Gateway web interface is supported by a CivetWeb web server. Web server settings are stored in a web server profile. A web server profile binds a CivetWeb configuration file to a security certificate. Kaspersky IoT Secure Gateway is delivered with a predefined profile that includes a security certificate signed by Kaspersky.

Viewing web server profiles

To view the list of web server profiles:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Settings** section.

7. Select the **Web server** tab.

You will see a list of created web server profiles.

Configuring Syslog

Kaspersky IoT Secure Gateway includes a Syslog client that you can use to send Syslog messages regarding events on devices in your network to a Syslog server. A Syslog client is managed through the Kaspersky Security Center Web Console.

To configure forwarding of Syslog messages to a Syslog server:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Settings** section.

7. Select the **Syslog** tab.

8. Set the toggle button in the upper part of the window to **Syslog enabled**.

9. Specify the Syslog server settings:

- In the **IP address** field, specify the IP address of the Syslog server.
- Specify the port in the **Port** field.
- In the drop-down list, select one of the following **Mode** options:
 - **UPD**.
 - **TCP**.
 - **TLS**.

10. Click the **Download certificate** button.

This opens a window for downloading a file to the system.

11. In the opened window, select the certificate.

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

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

To delete a certificate:

1. Under the description of the certificate that you want to delete, click the **Remove certificate** button.
2. Click **Save** in the lower part of the page to save the changes.

Configuring push notifications through the Kaspersky Security Center Web Console

Kaspersky IoT Secure Gateway can send push notifications to authorized devices. You can authorize your devices through the Kaspersky Security Center Web Console.

To enable forwarding of push notifications to a device:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Settings** section.
7. Select the **Push notifications** tab.
8. In the **Device name** field, enter the name that will be used by the system to send push notifications.
9. In the **Authorization key** field, enter the Firebase authorization code.
10. Click the **Download certificate** button.
This opens a window for downloading a file to the system.
11. In the opened window, select the certificate.
The file will be uploaded to the system and will appear in the profile.
12. Click **Save** in the lower part of the page to save the changes.

Configuring the date and time

To configure the date and time:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.

2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Settings** section.

7. Select the **Time** tab.

8. In the **Date** block, specify the system date.

9. In the **Time** block, specify the system time.

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

Indicate the current time in the UTC time zone.

Configuring a password policy

To change the password policy for new system users through the Kaspersky Security Center Web Console:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Settings** section.

7. Select the **Password policy** tab.

8. In the **Password policy profile** drop-down list, select the necessary policy: **Low security**, **Medium security**, or **High security**.

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

Configuring synchronization with Kaspersky Security Center

To configure the time of synchronization (heartbeat) with Kaspersky Security Center:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Settings** section.
7. Select the **KSC: Heartbeat** tab.
8. In the **Heartbeat** drop-down list, select the interval at which Kaspersky IoT Secure Gateway will synchronize with Kaspersky Security Center.
9. Click **Save** in the lower part of the page to save the changes.

Configuring masquerading

Masquerading is a type of network address translation whereby the sender's address is dynamically substituted depending on the address assigned to the specific interface.

To enable masquerading:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Settings** section.

7. Select the **NAT** tab.

8. Set the masquerading toggle to the appropriate position:

- **Masquerading enabled** if you need to enable masquerading.
- **Masquerading disabled** if you need to disable masquerading.

Regardless of the selected position of the masquerading toggle, routing of transit IP packets always remains enabled.

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

Restarting and updating software

You can update or restart Kaspersky IoT Secure Gateway through the Kaspersky Security Center Web Console.

To update Kaspersky IoT Secure Gateway:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.
2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".
The computer properties window opens.
3. Select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway.
This opens a window containing information about Kaspersky IoT Secure Gateway.
5. Select the **Application settings** tab.
6. Select the **Settings** section.
7. Select the **KSC Commands** tab.
8. Select the **Update** tab.
9. In the **Update server address** field, specify the address of the update package for Kaspersky IoT Secure Gateway in the following format: `https://<server IP address>/path_to_update_package` (for example, `https://10.10.10.10/update.pkg`).
10. In the **Command** drop-down list, select **Update**.
11. Click the **Save** button in the lower part of the page.
Kaspersky IoT Secure Gateway updates will be loaded.

To restart Kaspersky IoT Secure Gateway:

1. In the main window of the Kaspersky Security Center Web Console, select **Devices** → **Managed devices**.

2. Click the name of the computer where Kaspersky IoT Secure Gateway is running. If you do not see the computer name in the list, add it to the **Managed devices** group as described in the section titled "[Configuring how events are displayed in the Kaspersky Security Center Web Console](#)".

The computer properties window opens.

3. Select the **Applications** tab.

4. Click on Kaspersky IoT Secure Gateway.

This opens a window containing information about Kaspersky IoT Secure Gateway.

5. Select the **Application settings** tab.

6. Select the **Settings** section.

7. Select the **KSC Commands** tab.

8. In the **Command** drop-down list, select the **Restart** command.

9. Click the **Save** button in the lower part of the page.

Kaspersky IoT Secure Gateway will be restarted.

Contacting Technical Support

If you do not find a solution to your problem in the documentation for Kaspersky IoT Secure Gateway, you are advised to contact Kaspersky Technical Support. Technical Support experts will answer your questions about installing and using the system.

To receive additional information about the status of network interfaces and the routing table, you can go to the troubleshooting page in the [web interface](#). The page can be found here: <Kaspersky IoT Secure Gateway web interface address>/troubleshooting.html.

Information is displayed on the page <Kaspersky IoT Secure Gateway web interface address>/troubleshooting.html only if you have already logged in to the web interface under your user account.

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

- Call +7 (495) 780-33-67.

Calling by phone will allow you to consult with Technical Support experts in the local language.

- Send an email message to the Technical Support address: tasupport@kaspersky.com.

Glossary

Event

A record containing information about the detection of data in the system or internal network that requires the attention of an employee responsible for data security in your organization. An event is stored in the memory of the built-in computer Advantech UTX-3117.

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 entity

A part of Kaspersky IoT Secure Gateway that is designed to provide system functionality (such as authentication).

Kaspersky Security Center Web Console

Web application designed to manage the status of the security system of an enterprise network that is protected by Kaspersky applications.

KasperskyOS

A microkernel operating system used for building secure solutions.

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.

Password policy

A function that implements a specific rule regarding the complexity of new passwords.

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt residing on the 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.

Eclipse Mosquitto is a trademark of Eclipse Foundation, Inc.

Google Chrome and Firebase are trademarks of Google, Inc.

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

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

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