Kaspersky IoT Secure Gateway 1000

Contents

About Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 (also referred to as "the system") is a cyberimmune information system based on the KasperskyOS operating system with a preconfigured set of application software. Kaspersky IoT Secure Gateway 1000 is installed on an Advantech UTX-3117-S6A1N embedded computer and is designed to serve as a secure gateway for the Internet of Things in an enterprise network.

Kaspersky IoT Secure Gateway 1000 performs the following functions:

- Receives, scans, and distributes messages of sensors and other devices transmitted over the MQTT protocol.
- Registers 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 1000 can also operate as a firewall and DHCP server, and provide network address translation (NAT).

You can manage Kaspersky IoT Secure Gateway 1000 through the local web interface or remotely by using the web plug-in for the Kaspersky Security Center 13.2 Web Console.

Distribution kit

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

- Installation image for Kaspersky IoT Secure Gateway 1000: kisg-<application version number>-ru-en.tgz.
- Archive containing the installation image for the Kaspersky Security Center 13.2 Web Console web plug-in and signature file: WEB_Plugin_KISG_<plug-in version number>.zip.
- File containing third party code information (Legal Notices).
- Online Help.
- Version information (Release Notes).

Hardware and software requirements

The USB ports of the Advantech UTX-3117-S6A1N can be used only to connect a keyboard and mouse during initial configuration of Kaspersky IoT Secure Gateway 1000 or a bootable USB drive during installation of Kaspersky IoT Secure Gateway 1000. Connecting other devices to the Advantech UTX-3117-S6A1N through USB ports is not permitted.

Kaspersky IoT Secure Gateway 1000 requirements

Kaspersky IoT Secure Gateway 1000 can be installed only to the embedded Advantech UTX-3117FS-S6A1N computer.

The connection to the Kaspersky IoT Secure Gateway 1000 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 88 or later.
- Mozilla™ Firefox™ version 78 or later.

Requirements for Kaspersky Security Center components

To connect to Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console, Kaspersky Security Center version 13.2 must be installed in the local network of your organization.

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

- Kaspersky Security Center 13.2 Administration Server
- Kaspersky Security Center 13.2 Web Console

> Kaspersky Security Center 13.2 and Kaspersky Security Center 13.2 Web Console are not included in the Kaspersky IoT Secure Gateway 1000 distribution kit. They must be installed separately.

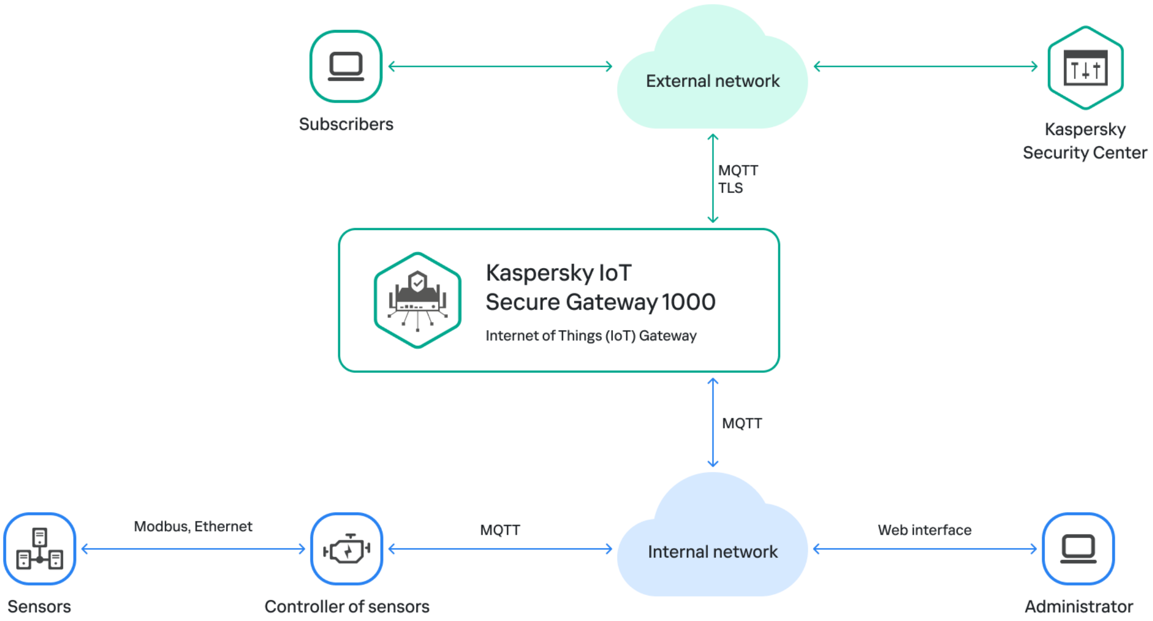
For information on installing Kaspersky Security Center 13.2 components, please refer to the Online Help Guide for Kaspersky Security Center.

Standard deployment of Kaspersky IoT Secure Gateway 1000

The standard deployment scenario for Kaspersky IoT Secure Gateway 1000 (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 1000 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 13.2 Web Console.



Standard deployment of Kaspersky IoT Secure Gateway 1000

Components of Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 includes the following components:

- *WEB Server*. Enables operation of the Kaspersky IoT Secure Gateway 1000 web interface.
- *MQTTbroker*. Provides Eclipse Mosquitto™ MQTT broker functionality.
- *Modem*. Provides for system event log data transfer using a cellular connection.
- *MQTT*. Provides forwarding of system events over the MQTT protocol (Message Queuing Telemetry Transport).
- *Syslog*. Provides forwarding of system events to a recipient Syslog server over the Syslog protocol.
- *Push*. Provides forwarding of system events using Firebase™ Cloud Messaging over the HTTPS protocol.
- *Firewall*. Provides firewall and connection control functionality.
- *Kaspersky Security Center*. Provides for centralized management of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.
- *DeviceDetection*. Provides for detection and categorization of devices on the network.
- *IPS*. Provides Intrusion Prevention functionality to protect against threats from an external network.
- *Update*. Provides updates of system entities.
- *DHCPserver*. Provides for DHCP server operations.

- *DHCPclient*. Provides for DHCP client operations.

- *Events& Audit*. Provides the capability to manage security events in Kaspersky IoT Secure Gateway 1000 and security events on the internal network.

Security recommendations for Kaspersky IoT Secure Gateway 1000

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

Physical security of equipment

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

- Restrict access to the room containing the hardware that has the application installed, and restrict access to the equipment of the dedicated network. Access to the room must be granted only to trusted persons, such as personnel who are authorized to install and configure the application.

- Employ technical resources or a security service to monitor physical access to equipment on which the application is running. Use security alarm equipment to monitor access to restricted rooms.

- Conduct video surveillance in restricted rooms.

Information security

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

- Ensure protection of traffic within the intranet system.

- Ensure that initial configuration of Kaspersky IoT Secure Gateway 1000 is performed only within the restricted perimeter.

- Use digital certificates that were published by trusted certificate authorities. If certificates have been potentially compromised, it is recommended to update them.

- Close the connection session with the Kaspersky IoT Secure Gateway 1000 web interface when the user is finished working in the web browser. To force termination of a connection session in the web browser, you need to use the **Log out** option in the user menu.

What's new

Kaspersky IoT Secure Gateway 1000 version 2.1 has the following new capabilities and improvements:

- Cyberimmunity – added functionality that allows Kaspersky IoT Secure Gateway 1000 to fulfill its security objectives and constraints ensuring that Kaspersky IoT Secure Gateway 1000 is a cyberimmune information system.
- Cellular connection to an external network – added support for the Huawei ME909s-120 v1 and v2 modem that enables Kaspersky IoT Secure Gateway 1000 to transmit data through cellular communication channels.
- Cellular connection settings management and monitoring – capability to create a new cellular connection profile and switch between profiles. You can manage cellular connection settings through the Kaspersky IoT Secure Gateway 1000 web interface and through the Kaspersky Security Center 13.2 Web Console.
- User authorization only with a certificate – added functionality that lets you connect to the Kaspersky IoT Secure Gateway 1000 web interface using an administrator certificate instead of user authorization with account credentials.
- User session renewal using a certificate – added functionality that lets you resume a connection to the Kaspersky IoT Secure Gateway 1000 web interface using the administrator certificate that was uploaded during authorization.
- Connection to Kaspersky Security Center using a certificate – added functionality that provides secure interaction between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center. Security is provided through the use of a KSC server certificate.
- Intrusion Detection System (IDS) – databases of Intrusion Detection rules have been updated. 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.
- Kaspersky IoT Secure Gateway 1000 event log – you can now export event log to a GZIP file via Kaspersky IoT Secure Gateway 1000 interface.
- Notification over the MQTT protocol – added functionality that lets you enable or disable forwarding of registered Kaspersky IoT Secure Gateway 1000 events over the MQTT protocol (Message Queuing Telemetry Transport) through the Kaspersky IoT Secure Gateway 1000 web interface and through the Kaspersky Security Center 13.2 Web Console.

Enabling and disabling the Advantech UTX-3117FS-S6A1N device

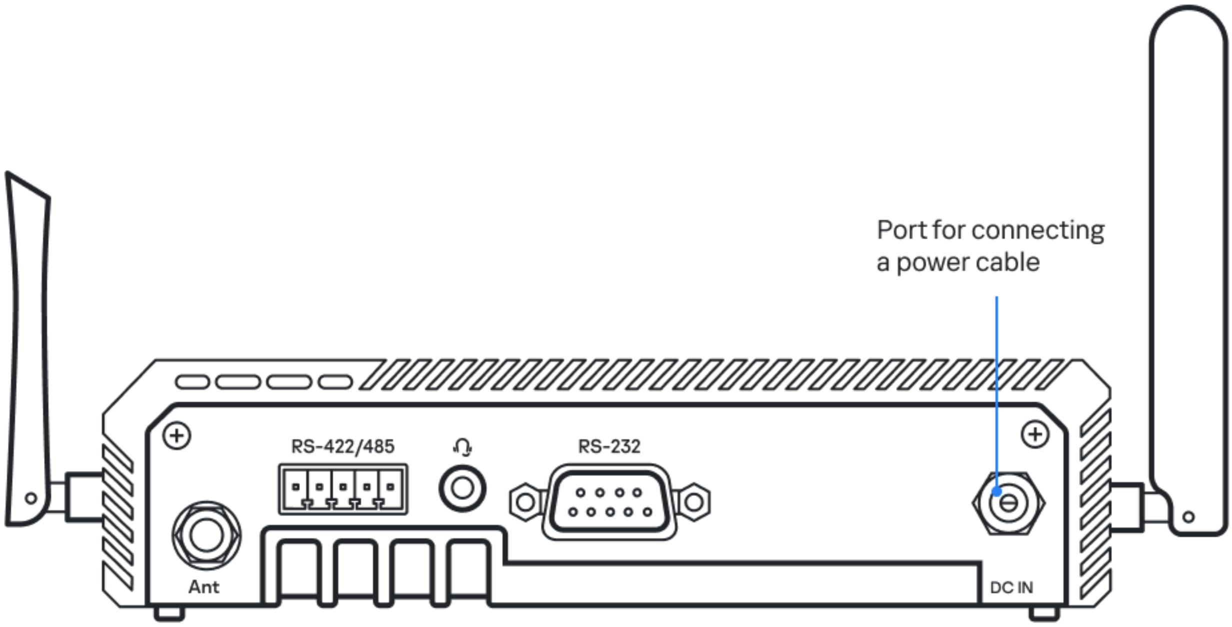
Before you start working with Kaspersky IoT Secure Gateway 1000, you must connect the Advantech UTX-3117FS-S6A1N device to the network and turn it on.

Preparations for installation and the actual installation of Kaspersky IoT Secure Gateway 1000 are performed by Kaspersky experts.

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

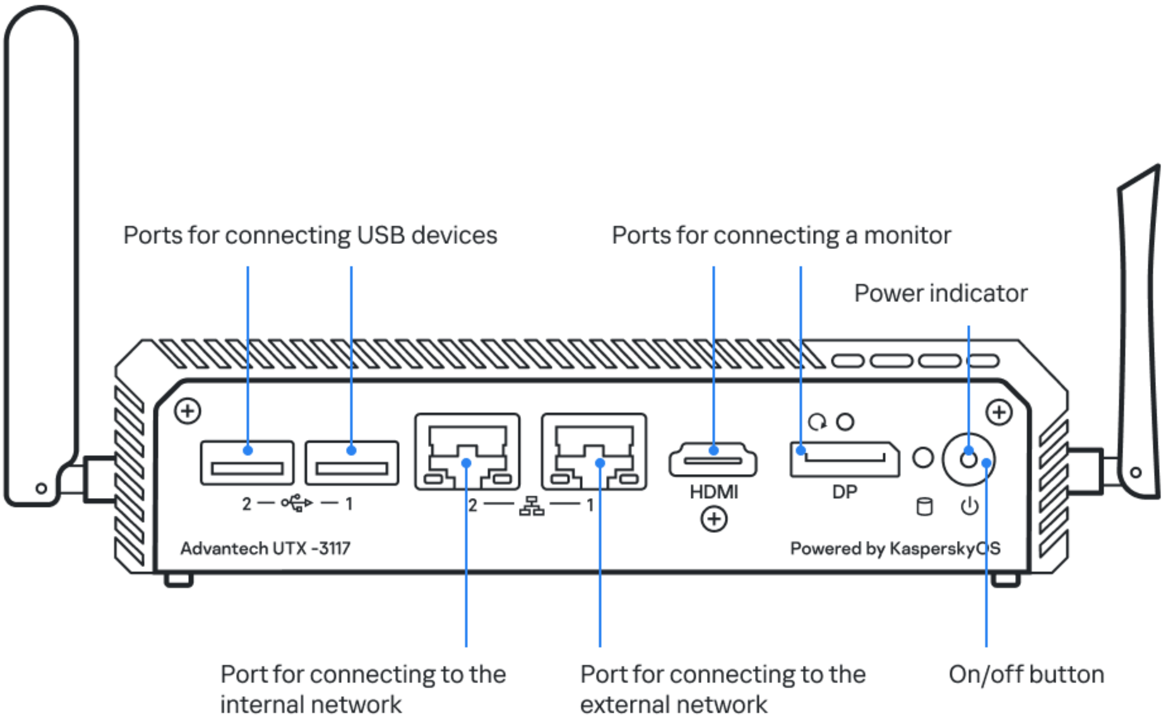
To turn on the Advantech UTX-3117FS-S6A1N device:

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 corresponding external network port on the front panel of the Advantech UTX-3117FS-S6A1N (see the figure below).


Ports for connecting USB devices
Ports for connecting a monitor
Power indicator
2 — — 1
2 — — 1
HDMI
DP
Advantech UTX -3117
Powered by KasperskyOS
Port for connecting to the internal network
Port for connecting to the external network
On/off button

Front panel of the Advantech UTX-3117

3. If you need to turn on the Advantech UTX-3117FS-S6A1N device, click the on/off button in the right part of the front panel.

   The Advantech UTX-3117FS-S6A1N will turn on, and Kaspersky IoT Secure Gateway 1000 will start automatically.

4. If you need to turn off the Advantech UTX-3117FS-S6A1N device, close the connection session with the Kaspersky IoT Secure Gateway 1000 web interface and click the on/off button in the right part of the front panel.

   The Advantech UTX-3117FS-S6A1N will shut down.

Connecting to the Kaspersky IoT Secure Gateway 1000 web interface

You can connect to the Kaspersky IoT Secure Gateway 1000 web interface using any supported browser. The browser must be installed on a computer that has access to Kaspersky IoT Secure Gateway 1000 through the internal network.

Kaspersky IoT Secure Gateway 1000 is delivered with a statically configured IP address of 192.168.1.1.

The DHCP server will be enabled by default in Kaspersky IoT Secure Gateway 1000. When you connect your computer to the network that Kaspersky IoT Secure Gateway 1000 is connected to through the internal network connection port, your computer will receive an IP address automatically.

To prevent errors when checking the administrator certificate validity term, it is recommended to make sure that the correct date and time are set in the device settings.

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

1. Open your browser.
2. If you are connecting to the Kaspersky IoT Secure Gateway 1000 web interface for the first time, add the private key that was created together with the administrator certificate in your browser. For more details about adding a key file to your browser, please refer to the relevant documentation on the browser you are using.
3. In your browser's address bar, enter the IP address of Kaspersky IoT Secure Gateway 1000: 192.168.1.1.

   The Kaspersky IoT Secure Gateway 1000 login page opens.
4. If you are connecting to the Kaspersky IoT Secure Gateway 1000 web interface for the first time, upload an administrator certificate. To do so, click the **Upload** button on the right of the name of the relevant type of certificate, and select a certificate file in CRT, CER, DER or PEM format.

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

   An administrator certificate and its private key must be uploaded before you connect to Kaspersky IoT Secure Gateway 1000 web interface.

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

   The specified certificates will not need to be uploaded again for subsequent connections to the Kaspersky IoT Secure Gateway 1000 web interface. Instead, the browser will prompt you to select a key for the already uploaded certificates.
5. If you need to manage the application through the Kaspersky Security Center 13.2 Web Console, upload a Kaspersky Security Center server certificate. To do so, click the **Upload** button on the right of the name of the

relevant type of certificate, and select a certificate file in CRT, CER, DER or PEM format. You can upload this certificate later.

> If there is no KSC server certificate in the system, it is not possible to configure the settings for connecting to Kaspersky Security Center.

6. Click the **Log in** button.

The browser window will display the Kaspersky IoT Secure Gateway 1000 web interface page.

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

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

> If you close the browser window without first closing the connection session, the session remains active. An unclosed session remains active for 5 minutes. During this time, the system can grant access to the Kaspersky IoT Secure Gateway 1000 web interface without prompting for a new administrator certificate, provided that the connection uses the same computer and browser.

To close or resume a connection session with the Kaspersky IoT Secure Gateway 1000 web interface:

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

   Your browser window will display the page for resuming your connection session with the Kaspersky IoT Secure Gateway 1000 web interface.

For additional security, a Kaspersky IoT Secure Gateway 1000 web interface connection session is closed if the system is idle for five minutes. You can resume a connection session with the Kaspersky IoT Secure Gateway 1000 web interface by clicking the **Log in** button on the page for resuming a connection session with the Kaspersky IoT Secure Gateway 1000 web interface.

Kaspersky IoT Secure Gateway 1000 web interface

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

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

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

Sections of the application web interface

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

- **Dashboard**. In this section, you can view summary information about system operation, including the latest events, detected devices, and the state of system entities.
- **Events**. In this section, you can view network security events that have occurred during the current session of the user's connection to the system through a browser. Network security events include detection of devices in the network, and any attempts to connect to the Kaspersky IoT Secure Gateway 1000 web interface.
- **Audit**. In this section, you can view the audit log of Kaspersky IoT Secure Gateway 1000.
- **Devices**. In this section, you can view a list of devices detected on the internal network, add trusted devices to the allowlist, and delete devices from the allowlist.
- **MQTT broker**. In this section, you can view and change the settings in the MQTT broker profile.
- **Settings**. This section contains the following tabs where you can view and change system settings:
  - **Network**. On this tab, you can configure the settings of the internal network and external network of Kaspersky IoT Secure Gateway 1000, and configure the cellular connection settings.
  - **System security**. On this tab, you can manage certificates of the administrator of Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center server.
  - **Web server**. On this tab, you can manage web server profiles.
  - **Utilities**. On this tab, you can view and change the settings of push notifications and MQTT notifications, and configure the settings for forwarding network security and audit logs to a recipient Syslog server.
  - **General**. On this tab, you can view and change the date and time settings of Kaspersky IoT Secure Gateway 1000.
  - **Kaspersky Security Center**. On this tab, you can view and change the address for connecting to the Kaspersky Security Center server.
- **About**. This section contains information about the version of Kaspersky IoT Secure Gateway 1000 installed on your device, and links to Online Help and third-party code information.

Workspace of the application web interface window

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

User menu

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

- Change the web interface language.
- Log out.

Security objectives and constraints

A *cyberimmune information system is* a system that guarantees the fulfillment of specific security objectives in all possible scenarios of system usage as stipulated by the developers.

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

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

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

Security objectives

Kaspersky IoT Secure Gateway 1000 has the following security objectives:

- Kaspersky IoT Secure Gateway 1000 provides a secure (confidentiality and integrity) communication channel from a device to digital platforms (Yandex IOT Core, Microsoft® Azure IoT hub) to transfer data received from IoT devices located in the internal network.
- Kaspersky IoT Secure Gateway 1000 provides for secure updates of the system version. Only updates signed by Kaspersky can be installed, including when updates are obtained through untrusted communication channels.
- Kaspersky IoT Secure Gateway 1000 ensures that system settings and configuration files are securely received (from a trusted source) and securely stored.
- Kaspersky IoT Secure Gateway 1000 accumulates and securely stores security events of a device (Secure audit: restart, update, information security events) and securely transmits them to Kaspersky Security Center.
- Kaspersky IoT Secure Gateway 1000 provides the capability for system administration from the internal network after user authorization via certificate when a secure channel is established.

Security constraints

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

- Kaspersky IoT Secure Gateway 1000 can be deployed in two ways:
  - With support for management through Kaspersky Security Center residing in the internal or external network. Kaspersky Security Center is a trusted source for receiving settings and configuration files of Kaspersky IoT Secure Gateway 1000.
  - Without support for management through Kaspersky Security Center. During deployment, you must compile a list of certificates that can be used by the administrator to connect to the Kaspersky IoT Secure Gateway 1000 web interface. The Kaspersky IoT Secure Gateway 1000 web interface is a trusted source for receiving settings and configuration files of Kaspersky IoT Secure Gateway 1000.
- Initial configuration of Kaspersky IoT Secure Gateway 1000 settings must be conducted under conditions that eliminate any possibility of a compromised Kaspersky Security Center.

- Kaspersky Security Center is considered to be trusted if Kaspersky IoT Secure Gateway 1000 is configured to interact with Kaspersky Security Center using a Kaspersky Security Center server certificate. Threats associated with a compromised Kaspersky Security Center are not considered.

- The device on which Kaspersky IoT Secure Gateway 1000 is installed has separate ports for connecting to the internal network and external network.

- The device on which Kaspersky IoT Secure Gateway 1000 is installed is operating in an environment that completely eliminates the possibility of any physical access by a cybercriminal, including their inability to directly connect to the device.

- A medium level of threat (basic elevated) from the external network is assumed.

- A low level of threat (basic) from the internal network is assumed.

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

- Threats associated with a vulnerability of the hardware platform are not considered.

- Threats associated with breached confidentiality, violated integrity or loss of data during its transmission from devices in the internal network to Kaspersky IoT Secure Gateway 1000 are not considered.

- The following threats associated with breached availability of the infrastructure are not considered:

  - Communication channels between the sides of network interaction

  - Kaspersky Security Center server

  - Digital platforms

Processing and storing data in Kaspersky IoT Secure Gateway 1000

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

Data provision

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

Each time Kaspersky IoT Secure Gateway 1000 is started, it deletes the network security log and the list of devices detected in the network that are not included in the list of allowed devices. When a device is restarted or a connection is terminated, the network security log and the list of detected devices will be reset. All certificate details are stored in a separately allocated space on the drive.

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

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

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

When devices are detected in the enterprise network, the device name may contain personal data of the user. You need to rename a device when adding it to the allowlist.

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

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

- Network security log.
- Audit log.
- Set of rules of the Intrusion Prevention System (IPS).
- IP addresses, MAC addresses, and network device names that are on the list of allowed devices.
- MQTT broker settings:
  - Indicator of whether the profile can be edited
  - Indicator of whether the profile is active

  - Profile name
  - CA certificate for the MQTT server (the certificate may be self-signed)
  - Client certificate for the MQTT server
  - Private key for the client certificate of the MQTT server
  - Information about configuration files: file name, file type, file contents
- General settings of Kaspersky IoT Secure Gateway 1000:
  - LAN settings:
    - IP address of Kaspersky IoT Secure Gateway 1000 within the internal network:
    - Subnet mask
    - DHCP server settings:
      - DHCP server usage (enabled or disabled)
      - Start and end of IP address range
      - Primary DNS server address
      - Secondary DNS server address
  - WAN settings:
    - DHCP client usage (enabled or disabled)
    - IP address
    - Subnet mask
    - Default network gateway
    - Primary DNS server address
    - Secondary DNS server address
  - Cellular connection settings of Kaspersky IoT Secure Gateway 1000:
    - Use of the modem as the main communication channel (enabled or disabled)
    - Modem DNS server addresses
    - Data on communication provider profiles:
      - Indicator of whether the profile is active
      - Indicator of whether the profile can be edited
      - Profile name

    - Data on the profile configuration file: file name, file type, file contents
- Kaspersky IoT Secure Gateway 1000 security settings:
  - Administrator certificate for connecting to the Kaspersky IoT Secure Gateway 1000 web interface
  - KSC server certificate
- Kaspersky IoT Secure Gateway 1000 web server settings:
  - Indicator of whether the profile can be edited
  - Indicator of whether the profile is active
  - Profile name
  - Configuration files
  - Web server certificate
  - Private key of the web server certificate
- Settings of Syslog notifications:
  - Use of notifications for the Syslog server (enabled or disabled)
  - IP address and port of the Syslog server
  - Notification forwarding mode: UDP, TCP, TLS
  - Syslog server certificate
- Settings of push notifications:
  - Name of the device that will receive push notifications
  - Authorization key of the device that will receive push notifications
  - Google™ FCM server certificate for push notifications
- Settings of MQTT notifications:
  - Use of notifications over the MQTT protocol (enabled or disabled)
  - MQTT server address and port
  - MQTT-topic name
  - Use of authentication when sending notifications over the MQTT protocol (enabled or disabled)
  - User name and password
  - Use of a secure SSL connection (enabled or disabled)
  - CA certificate for sending notifications over the MQTT protocol

    - Client certificate for sending MQTT notifications
    - Private key of the client certificate for sending MQTT notifications
  - Kaspersky IoT Secure Gateway 1000 date and time settings
  - Settings for connecting to the Kaspersky Security Center server: server address and port
- Kaspersky IoT Secure Gateway 1000 version information

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

- MQTT broker settings:
  - Indicator of whether the profile can be edited
  - Indicator of whether the profile is active
  - Profile name
  - CA certificate for the MQTT server (the certificate may be self-signed)
  - Client certificate of the MQTT server
  - Private key for the client certificate of the MQTT server
  - Information about configuration files: file name, file type, file contents
- Network settings of Kaspersky IoT Secure Gateway 1000:
  - LAN settings:
    - IP address of Kaspersky IoT Secure Gateway 1000 within the internal network:
    - Subnet mask
    - DHCP server settings:
      - State of the DHCP server (enabled or disabled)
      - Start and end of IP address range
      - Primary DNS server address
      - Secondary DNS server address
  - WAN settings:
    - State of the DHCP client (enabled or disabled)
    - IP address
    - Subnet mask
    - Default network gateway

        - Primary DNS server address
        - Secondary DNS server address
    - Settings of firewall rules:
        - List of rules
        - State of a rule (enabled or disabled)
        - Action that the firewall must take on network traffic that matches a rule
        - Zone to which the rule is applied
        - IP address of the traffic source
        - Port of the traffic source, if this setting is applicable to the utilized protocol
        - IP address of the traffic destination
        - Port of the traffic destination, if this setting is applicable to the utilized protocol
        - Utilized protocol
    - Settings of the Intrusion Prevention System:
        - Use of the Intrusion Prevention System (enabled or disabled)
        - Availability of the Intrusion Prevention System
        - IP addresses that were entered into the list of denied IP addresses
        - Use of a list of denied IP addresses (when the list of denied IP addresses is disabled, attacks will be detected but the IP addresses from which the attacks originated will not be blocked)
        - IDs of signatures used for adding IP addresses to the list of denied IP addresses
        - IP addresses that were entered into the list of allowed IP addresses
    - Masquerading settings: state of masquerading (enabled or disabled)
- Kaspersky IoT Secure Gateway 1000 settings:
    - Kaspersky IoT Secure Gateway 1000 web server settings:
        - Indicator of whether the profile can be edited
        - Indicator of whether the profile is active
        - Profile name
    - Kaspersky IoT Secure Gateway 1000 date and time settings
    - Cellular connection settings of Kaspersky IoT Secure Gateway 1000:
        - Modem operating status

        - Modem signal strength
        - Use of the modem as the main communication channel (enabled or disabled)
        - Modem DNS server addresses
        - Data for communication providers:
            - Indicator of whether the configuration file is active
            - Indicator of whether the configuration file can be edited
            - Configuration file type
            - Configuration file name
            - Configuration file contents
    - Kaspersky IoT Secure Gateway 1000 security settings:
        - Administrator certificate for connecting to the Kaspersky IoT Secure Gateway 1000 web interface
        - KSC server certificate
- Settings for forwarding Syslog notifications:
    - Forwarding of notifications to the Syslog server (enabled or disabled)
    - IP address and port of the Syslog server
    - Notification forwarding mode: UDP, TCP, TLS
    - Syslog server certificate
- Settings for forwarding push notifications:
    - Name of the device that will receive push notifications
    - Authorization key
    - Google FCM server certificate for forwarding push notifications
- Settings for forwarding MQTT notifications:
    - Forwarding of notifications over the MQTT protocol (enabled or disabled)
    - MQTT server address and port
    - MQTT-topic name
    - Use of authentication when sending notifications over the MQTT protocol (enabled or disabled)
    - User name and password
    - Use of a secure SSL connection (enabled or disabled)

  - CA certificate for sending MQTT notifications
  - Client certificate for sending MQTT notifications
  - Private key of the client certificate for sending MQTT notifications
- Settings for interaction between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 13.2 Web Console:
  - Synchronization period for synchronizing the settings of Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 13.2 Web Console
  - List of commands that the Kaspersky Security Center 13.2 Web Console can send to Kaspersky IoT Secure Gateway 1000
  - Kaspersky IoT Secure Gateway 1000 update address
- Kaspersky IoT Secure Gateway 1000 version information

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

About storing Kaspersky IoT Secure Gateway 1000 logs

Kaspersky IoT Secure Gateway 1000 saves data on audit and network security events. Depending on the type of log used for saving data, Kaspersky IoT Secure Gateway 1000 uses the following storage methods:

- Data block of specific disk sectors.

  The contents of the audit log are stored in a data block of specific disk sectors. You can view the audit log through the Kaspersky IoT Secure Gateway 1000 web interface or save it to the local computer.

- Device memory.

  The contents of the network security log are stored in the device memory. You can view the network security log through the Kaspersky IoT Secure Gateway 1000 web interface or through the Kaspersky Security Center 13.2 Web Console.

Kaspersky IoT Secure Gateway 1000 lets you save a log of all events to a file. You can use the Kaspersky IoT Secure Gateway 1000 web interface to save a file containing a log of all events to the local computer.

If necessary, you can also configure forwarding of data from the audit and network security event log via MQTT, Syslog, and push notifications.

Licensing Kaspersky IoT Secure Gateway 1000

The Terms of Use of the application are set forth in the End User License Agreement provided for this specific application.

Configuring Kaspersky IoT Secure Gateway 1000

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

Scenario: Quick Start for administrators

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

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

1. **Installing Kaspersky Security Center**

   Download the Kaspersky Security Center 13.2 distribution package and install the full version of Kaspersky Security Center on the server. The distribution package of the full version of Kaspersky Security Center 13.2 includes the Kaspersky Security Center 13.2 Web Console. You are advised to select the standard installation. For detailed information on installing Kaspersky Security Center, please refer to the *Main installation scenario* section of the Kaspersky Security Center 13.2 Online Help Guide.

2. **Configuring firewall rules**

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

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

   In the Kaspersky Security Center 13.2 Web Console interface, install the Kaspersky IoT Secure Gateway 1000 administration web plug-in. A ZIP archive containing the distribution package for the Kaspersky IoT Secure Gateway 1000 web plug-in is included in the distribution kit.

4. **Configuring connection of UEFI protection devices**

   On the Kaspersky Security Center Administration Server, enable use of port 13294 for the TCP protocol to configure the connection between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center. For detailed information on enabling port 13294 on the Kaspersky Security Center Administration Server, please refer to the *UEFI protection devices* section of the Kaspersky Security Center 13.2 Online Help Guide.

5. **Installing Kaspersky IoT Secure Gateway 1000**

   Complete preparations for installation and then install Kaspersky IoT Secure Gateway 1000 on the Advantech UTX-3117FS-S6A1N device.

6. **Connecting to the Kaspersky IoT Secure Gateway 1000 web interface**

   Connect to the Kaspersky IoT Secure Gateway 1000 web interface. An administrator certificate and a private key must be created in advance. The private key must be added to the browser used to connect to the Kaspersky IoT Secure Gateway 1000 web interface. For more details about adding a private key file to your browser, please refer to the relevant documentation on the browser you are using.

7. **Configuring Kaspersky IoT Secure Gateway 1000 settings**

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

   - Connection to the external network and internal network
   - Modem profile

8. **Creating and uploading a Kaspersky Security Center server certificate**

   Create a new Kaspersky Security Center server certificate and save it on the local device. In the Kaspersky IoT Secure Gateway 1000 web interface, upload the Kaspersky Security Center server certificate for configuring a connection to the Kaspersky Security Center 13.2 Web Console.

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

   In the Kaspersky IoT Secure Gateway 1000 web interface, configure the connection to Kaspersky Security Center.

10. **Adding Kaspersky IoT Secure Gateway 1000 to the list of managed devices**

    Connect to the Kaspersky Security Center 13.2 Web Console and add Kaspersky IoT Secure Gateway 1000 to the list of managed devices in Kaspersky Security Center.

11. **Creating an active Kaspersky Security Center policy for Kaspersky IoT Secure Gateway 1000**

    Create an active policy for Kaspersky IoT Secure Gateway 1000. An active policy is required so that Kaspersky Security Center can receive Kaspersky IoT Secure Gateway 1000 event logs. For detailed information on creating a policy, refer to the *Creating a policy* section in the Kaspersky Security Center 13.2 Online Help.

When these actions are complete, Kaspersky IoT Secure Gateway 1000 will be ready for operation. You will be able to manage Kaspersky IoT Secure Gateway 1000 through the Kaspersky IoT Secure Gateway 1000 web interface or through the Kaspersky Security Center 13.2 Web Console, and monitor devices and events in the network.

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

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

> Prior to performing the configuration, you must make sure that the port that will be used to connect to an internal network device is accessible for the connection.

The access configuration scenario consists of the following steps:

1. **Configuring routing of transit IP packets**

   On the device residing in the external network, configure routing of transit IP packets so that the network packets intended for the internal network device that needs to be accessed are forwarded through the external network interface of Kaspersky IoT Secure Gateway 1000 (WAN).

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

2. **Disabling masquerading**

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

3. **Creating a rule for a device in an external network**

   Create a firewall rule that opens the external interface of Kaspersky IoT Secure Gateway 1000 (WAN) to allow network packets to pass from the external network device to a device in the internal network.

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

4. **Creating a rule for a device in the internal network**

   Create a firewall rule that opens the internal interface of Kaspersky IoT Secure Gateway 1000 (LAN) to allow network packets to pass from an internal network device to a device in an external network.

5. **Check the connection to an internal network device.**

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

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

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

Configuring network settings

Kaspersky IoT Secure Gateway 1000 is delivered with a statically configured IP address of 192.168.1.1. 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 network.

An *external network* is a network used by Kaspersky IoT Secure Gateway 1000 to access the Internet or to interact with Kaspersky Security Center.

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

You can view and change the network settings of Kaspersky IoT Secure Gateway 1000 under **Network** on the **Internal network** or **External network** tab.

The Kaspersky IoT Secure Gateway 1000 internal network can be used to carry out the following tasks:

- Connect to the Kaspersky IoT Secure Gateway 1000 web interface.
- Forward event logs to an internal Syslog server.
- Monitor devices that are connected to Kaspersky IoT Secure Gateway 1000.

The Kaspersky IoT Secure Gateway 1000 external network can be used to carry out the following tasks:

- Configure interaction between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center.
- Provide Intrusion Prevention functionality (IPS entity).
- Forward event logs to an external Syslog server.

Configuring the LAN settings

When the IP address of Kaspersky IoT Secure Gateway 1000 in the internal network is changed, the web interface connection session will be closed and you will be redirected to the page for resuming a connection session with the Kaspersky IoT Secure Gateway 1000 web interface.

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

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

To configure the LAN settings:

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

     The **MAC address** field displays the MAC address of the system in the internal network.
3. If you want to configure network settings automatically via DHCP for the devices in the internal network, set the **Use DHCP server** toggle button to Enabled and specify values for the following settings:
   - **Start of IP address range**.
   - **End of IP address range**.
   - **Primary DNS server address**.
   - **Secondary DNS server address**.

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

Configuring the WAN settings

To configure the WAN settings:

1. In the menu in the left part of the web interface page, select **Settings** → **Network**.
2. On the **WAN** tab, do one of the following:

- If you need to configure network settings automatically using the DHCP protocol, set the **Automatic (via DHCP)** toggle button to the enabled position. The **Automatic (via DHCP)** toggle button is switched on by default.

  > If the DHCP server issued null DNS server addresses to Kaspersky IoT Secure Gateway 1000 when enabling automatic configuration of external network settings, the IP address 208.67.222.222 (OpenDNS server) will be used by default to convert a domain name to an IP address.

- If you need to manually configure the network settings, set the **Automatic (via DHCP)** toggle button to the disabled position and specify the values for the following settings:

  - **IP address**.
  - **Subnet mask**.
  - **Gateway**.
  - **Primary DNS server address**.
  - **Secondary DNS server address**.

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

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

4. Restart Kaspersky IoT Secure Gateway 1000 to apply the changes to the network settings.

Configuring the settings for connecting to Kaspersky Security Center

To securely manage Kaspersky IoT Secure Gateway 1000 from the Kaspersky Security Center 13.2 Web Console, you must configure the Kaspersky Security Center connection settings.

> If there is no KSC server certificate in the system, it is not possible to configure the settings for connecting to Kaspersky Security Center.

To configure the settings for connecting to Kaspersky Security Center:

1. In the menu in the left part of the web interface page, select **Settings** → **Kaspersky Security Center**.

   The **Kaspersky Security Center connection settings** window opens.

2. In the **Domain address** field, enter the domain address of the Kaspersky Security Center server to which you need to connect.

   The **Port** field indicates the port number used for the connection.

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

Configuring cellular connection settings

> If a device does not have a modem, the use of a cellular connection and configuration of cellular connection settings are unavailable.

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

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

Modem profiles table

The system provides two types of modem profiles:

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

Information about modem profiles is provided in the **Profiles** table under **Settings** → **Network** → **Modem**. The table shows the following information for each modem profile:

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

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

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

Enabling and disabling a cellular connection

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

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

1. In the menu in the left part of the web interface page, select **Settings** → **Network**.
2. Go to the **Modem** tab. In the **Modem settings** block, move the **Use modem as main communication channel** toggle button to the necessary position to enable or disable use of the modem.
3. Click **Save** to save the changes made to the settings.
4. Restart Kaspersky IoT Secure Gateway 1000 to apply the changes to the settings.

Creating a modem profile

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

To create a new modem profile:

1. In the menu in the left part of the web interface page, select **Settings** → **Network**.
2. Select the **Modem** tab.

   This opens the **Modem settings** window, which contains a table of modem profiles in the lower part of the window.
3. Click the **Create new** button in the lower part of the page.

   The **Create modem profile** pane opens on the right.
4. In the **Template** drop-down list, select the modem profile that you want to use as the basis for creating the new profile. The modem configuration file of the selected profile is added to the new profile.

   If you want to create an empty profile, select **None** in the **Template** drop-down list. You can complete the empty modem profile at a later time.
5. In the **Name** field, enter the profile name using letters of the English alphabet.
6. Click **Save** in the lower part of the page to save the changes.

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

Copying a modem profile

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

To copy a previously created modem profile:

1. In the menu in the left part of the web interface page, select **Settings** → **Network**.
2. Select the **Modem** tab.

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

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

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

   The **Copy modem profile** pane opens.

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

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

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

Completing an empty modem profile

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

To complete an empty modem profile:

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

2. Select the **Modem** tab.

3. In the lower part of the page in the **Profiles** table, in the **Name** column, click the ⊞ icon next to the empty profile.

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

4. Create a modem configuration file by clicking the **Create new file** button.

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

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

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

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

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

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

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

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

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

10. Type the required modem configuration file settings in the text editor window.

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

Editing a modem profile

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

To change the name of a modem profile:

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

2. Select the **Modem** tab.

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

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

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

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

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

To change the modem profile settings:

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

2. Select the **Modem** tab.

3. In the lower part of the page, in the **Profiles** table, in the **Name** column, click the ⊞ icon next to the profile that you want to edit.

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

4. If you need to edit a configuration file, click the name of the configuration file and do the following in the **Edit modem configuration file** pane that opens on the right:

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

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

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

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

5. If you need to delete a configuration file, click the name of the configuration file and click the 🗑 icon located in the lower part of the **Edit modem configuration file** pane that opens on the right. Confirm file deletion.

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

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

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

Switching to a different modem profile

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

To switch to a different modem profile:

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

   The **Edit modem profile** pane opens on the right.
4. In the lower part of the pane, click the **Set as active** button.
5. Restart Kaspersky IoT Secure Gateway 1000 to apply the changes.

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

Deleting a modem profile

You can delete a modem profile in the Kaspersky IoT Secure Gateway 1000 web interface.

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

To delete a modem profile:

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

   The **Edit modem profile** pane opens on the right.
4. Click the 🗑 icon in the lower part of the pane and confirm profile deletion.

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

Managing the security of Kaspersky IoT Secure Gateway 1000

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

The following certificates are used in Kaspersky IoT Secure Gateway 1000:

- *Administrator certificate* for securely connecting to the Kaspersky IoT Secure Gateway 1000 web interface through a browser.
- *Kaspersky Security Center server certificate* for securely connecting to Kaspersky IoT Secure Gateway 1000 from the web interface of the Kaspersky Security Center 13.2 Web Console.
- *Certificate* for sending MQTT notifications, push notifications, and Syslog notifications about events registered by Kaspersky IoT Secure Gateway 1000.

It is recommended to update certificates in the following cases:

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

You can view previously uploaded certificates, add new certificates, or remove certificates from Kaspersky IoT Secure Gateway 1000.

Creating a KSC server certificate

A Kaspersky Security Center server certificate is required for securely connecting to Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

For detailed information about the requirements applied to Kaspersky Security Center server certificates, please refer to the section titled *Requirements for user certificates in Kaspersky Security Center* in the Kaspersky Security Center 13.2 Online Help Guide.

You can issue a new Kaspersky Security Center server certificate in the Kaspersky Security Center 13.2 Web Console.

To issue a new KSC server certificate through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Kaspersky Security Center 13.2 Web Console, click the 🔧 icon next to the name of the relevant Kaspersky Security Center Administration Server.

   The **Administration Server properties** window opens.

2. Select the **Certificates** section.

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

4. Click the **Reissue** button.

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

- Use old connection address

  > The address of the Administration Server to which Kaspersky IoT Secure Gateway 1000 connects will remain the same.
  >
  > This option is selected by default.

- Change connection address to

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

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

The new KSC server certificate will be issued.

To upload a Kaspersky Security Center certificate file in the Kaspersky IoT Secure Gateway 1000 web interface, the Kaspersky Security Center certificate file that was created through the web interface of the Kaspersky Security Center 13.2 Web Console must be saved on the local computer.

To save a Kaspersky Security Center certificate file that was created in the Kaspersky Security Center 13.2 Web Console:

1. In the web interface menu of the Kaspersky Security Center 13.2 Web Console, click the 🔧 icon next to the name of the relevant Kaspersky Security Center Administration Server.

   The **Administration Server properties** window opens.

2. Select the **Certificates** section.

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

4. Click the **Manage certificate** button.

5. In the opened pane on the right, in the **Connection address** block, click the IP address of Kaspersky IoT Secure Gateway 1000 for which the certificate was issued.

The certificate file will begin to automatically download.

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

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

A created Kaspersky Security Center server certificate file needs to be added to Kaspersky IoT Secure Gateway 1000 to configure a connection with Kaspersky Security Center.

Creating an administrator certificate

The *TLS protocol* (Transport Layer Security) is a secure protocol that uses encryption to transfer data in local networks and on the Internet. The TLS protocol is used in web applications to create secure connections between a client application and a web server.
The TLS protocol is used in Kaspersky IoT Secure Gateway 1000 to set up a secure communication channel between the Kaspersky IoT Secure Gateway 1000 web server and the browser that the user uses to connect to the Kaspersky IoT Secure Gateway 1000 web interface. When first connecting to the Kaspersky IoT Secure Gateway 1000 web interface, you must create and upload an administrator certificate. The uploaded administrator certificate will then be used for subsequent user authentication when connecting to the Kaspersky IoT Secure Gateway 1000 web interface again.

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

You can use the OpenSSL tool to create an administrator certificate.

To create an administrator certificate using the OpenSSL tool:

1. In the console, start the OpenSSL tool and run the following command:

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

   where:

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

- `CN` – certificate name.

2. Enter and confirm the password for the private certificate key.

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

   - `cert.pem` – administrator certificate file.
   - `cert_key.pem` – private key of the administrator certificate.

   The created administrator certificate file `cert.pem` must be loaded during the first authorization in Kaspersky IoT Secure Gateway 1000 web interface.

3. Run the following command in the console:

   ```
   openssl pkcs12 -export -in cert.pem -inkey cert_key.pem -out cert.p12 -name "cert_key"
   ```

4. Enter the password that you specified in step 2 of these instructions.

   As a result, the private key file `cert.p12` of the administrator certificate is created in the directory where the command was executed.

   The created private key file `cert.p12` of the administrator certificate must be added in the browser that you use to connect to the Kaspersky IoT Secure Gateway 1000 web interface. For more details about adding a private key file to your browser, please refer to the relevant documentation on the browser you are using.

Updating certificates

It is recommended to update the administrator certificate or Kaspersky Security Center server certificate in the following cases:

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

> When updating the administrator certificate in the Kaspersky IoT Secure Gateway 1000 web interface, you may need to restart the browser or clear the cache of the current user session in Kaspersky IoT Secure Gateway 1000.

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

To add or remove a certificate:

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

   This opens a window displaying the following information about certificates:

   - The **Administrator certificate** area shows data on the current administrator certificate.

- The **Kaspersky Security Center server certificate** area shows data on the current certificate of the Kaspersky Security Center server.

2. If you need to replace the administrator certificate with a new one, in the **Administrator certificate** block click the **Upload** button and select the certificate file in the opened window.

   Only files in the CRT, CER, DER, or PEM format can be added as a certificate.

   The new administrator certificate will upload to the system and the previously uploaded certificate will be deleted.

   > Kaspersky IoT Secure Gateway 1000 does not let you delete an administrator certificate without replacing the certificate with a new one.

3. If you need to add or delete a certificate previously uploaded to the Kaspersky Security Center server, complete one of the following steps in the **Kaspersky Security Center server certificate** block:

   - If you need to upload a Kaspersky Security Center server certificate, click the **Upload** button and select the certificate file in the open window.

     Only files in the CRT, CER, DER, or PEM format can be added as a certificate.

     The new Kaspersky Security Center server certificate will upload to the system and the previously uploaded certificate will be deleted.

   - If you need to delete the KSC server certificate, click the **Delete** button and confirm deletion.

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

Configuring MQTT broker settings

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

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

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

In the Kaspersky IoT Secure Gateway 1000 web interface menu, one of the following statuses of MQTT broker configuration is displayed next to the **MQTT broker** section:

- ✓ – means that the MQTT broker settings are configured correctly.

- ⚠ – means that the MQTT broker cannot connect to the network, so you need to configure the network settings.
- ❗ – means that the MQTT broker settings are configured incorrectly, so you need to configure the MQTT broker settings.

Table of MQTT broker profiles

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

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

Information about MQTT broker profiles is provided in the **Profiles** table in the **MQTT broker** section. The table shows the following information for each MQTT broker profile:

- 🔒 – profile editing access. This icon indicates that a profile is read-only and is only displayed for predefined profiles.
- **Active** – the ✅ icon indicates that the MQTT broker profile is currently being used in the application.
- **Name** – name of the profile.
- **Modified** – date and time of the most recent change in the profile.

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

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

Creating an MQTT broker profile

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

To create a new MQTT broker profile:

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

   This opens a table that lists the MQTT broker profiles.

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

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

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

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

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

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

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

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

Copying an MQTT broker profile

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

To copy a previously created MQTT broker:

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

   This opens a table that lists the MQTT broker profiles.

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

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

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

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

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

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

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

Completing an empty MQTT broker profile

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

To complete an empty MQTT broker profile:

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

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

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

3. If you are planning to use an MQTT broker profile to connect to devices or cloud services in an external network, upload the Certification Authority certificate, client certificate, and private key. To do so, click the **Upload** button in the lower part of the page. In the opened file upload window, select the relevant files. Repeat this step as many times as required to upload all necessary certificates and keys to the system. In Kaspersky IoT Secure Gateway 1000, you can only upload certificates in PEM format with the CRT extension, and keys in PEM format with the KEY extension. The size of each file must not exceed 131 KB.

   The uploaded files are displayed in the profile settings.

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

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

5. In the **Type** drop-down list, select the type of configuration file. The following options are available:

   - **Main configuration file**. This contains the main settings for MQTT broker operation. The main configuration file must be added to the MQTT broker profile so that this profile can be activated.

   - **Configuration file**. This contains additional settings for MQTT broker operation.

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

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

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

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

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

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

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

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

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

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

    > Kaspersky IoT Secure Gateway 1000 does not let you upload the main configuration file. This type of file can only be created.

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

Modifying an MQTT broker profile

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

To change the name of an MQTT broker profile:

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

   The **Profiles** table is displayed.

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

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

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

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

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

To change the settings of the MQTT broker profile:

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

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

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

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

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

   > Kaspersky IoT Secure Gateway 1000 does not let you upload the main configuration file. This type of file can only be created.

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

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

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

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

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

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

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

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

6. If you are planning to use an MQTT broker profile to connect to devices or cloud services in an external network, upload the Certification Authority certificate, client certificate, and private key. To do so, click the **Upload** button in the lower part of the page. In the opened file upload window, select the relevant files. Repeat this step as many times as required to upload all necessary certificates and keys to the system. In Kaspersky IoT Secure

Gateway 1000, you can only upload certificates in PEM format with the CRT extension, and keys in PEM format with the KEY extension. The size of each file must not exceed 131 KB.

The uploaded files are displayed in the profile settings.

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

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

Switching to a different MQTT broker profile

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

To switch to a different 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 broker 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, next to the selected profile the icon ✅ will appear. The profile is now active and will be used by Kaspersky IoT Secure Gateway 1000 when receiving data over the MQTT protocol.

Deleting an MQTT broker profile

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

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

To delete an MQTT broker profile:

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

   This opens the **Profiles** table that lists the MQTT broker profiles.

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

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

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

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

Limitations when configuring an MQTT broker

Connections to local devices are made without using a TLS protocol. Connections to devices on an external network are made using a TLS protocol.

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

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

  The following parameters are not supported when configuring a connection with Kaspersky IoT Secure Gateway 1000 from internal network: `cafile`, `certfile`, `ciphers_tls1.3`, `crlfile`, `dhparamfile`, `keyfile`, `require_certificate`, `tls_engine`, `tls_engine_kpass_sha1`, `tls_keyform`, `use_identity_as_username`, `use_subject_as_username`, `psk_hint`.
- It is required to use the TLS protocol for connection of Kaspersky IoT Secure Gateway 1000 with devices or cloud services in the external network.

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

Configuring the web server

Operation of the Kaspersky IoT Secure Gateway 1000 web interface is supported by a CivetWeb web server. Web server settings are stored in a web server profile. A web server profile binds a CivetWeb configuration file to a security certificate. Kaspersky IoT Secure Gateway 1000 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 1000 lets you create new profiles, edit existing profiles, and switch between profiles. Different profiles enable you to work with different security certificates. For the Kaspersky IoT Secure Gateway 1000 web interface to work, one of the web server profiles must be active. The predefined profile is active by default.

Table of web server profiles

Kaspersky IoT Secure Gateway 1000 provides for two types of web server profiles:

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

Information about web server profiles is provided in the **Profiles** table under **Settings** → **Web server**. The table shows the following information for each web server profile:

- 🔒 – web server profile editing access. This icon indicates that a profile is read-only and is only displayed for predefined profiles.
- **Active** – the ✓ icon indicates that the web server profile is currently being used in the application.
- **Name** – name of the web server profile.
- **Modified** – date and time of the most recent change in the profile.

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

- 🔒 – file editing access. This icon informing you that the file is read-only is displayed only for files of a predefined profile.
- **Type** – type of file.
- **Name** – name of the file.
- **Modified** – date and time of the most recent change of the file.

Creating a web server profile

You can create new web server profiles. Different web server profiles enable you to work with different security certificates.

To create a new web server profile:

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

   This opens a window showing the table of web server profiles.

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

   The **Create web server profile** pane opens on the right.

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

   The CivetWeb configuration file and security certificate of the selected profile are added to the new profile.

   If you want to create an empty profile, leave **None** selected in the **Template** drop-down list. You can complete the empty web server profile at a later time.

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

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

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

Copying a web server profile

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

To copy a previously created web server profile:

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

   This opens a window showing the table of web server profiles.

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

   The **Edit web server profile** pane opens on the right.

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

   The **Copy web server profile** pane opens.

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

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

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

Completing an empty web server profile

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

To complete an empty web server profile:

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

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

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

3. Add a security certificate to the web server profile by clicking the **Upload** button in the lower part of the page. In the opened file upload window, select a certificate file in PEM format with the CRT extension.

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

4. Add a security certificate key to the web server profile by clicking the **Upload** button in the lower part of the page. In the opened file upload window, select a key file in PEM format with the KEY extension.

   The key file is uploaded to the system and appears in the profile settings.

5. Create a configuration file in the web server profile by clicking the **Create new file** button.

   The **Create web server configuration file** pane opens on the right.

6. In the opened pane, in the **Name** field, enter the name of the configuration file using letters of the English alphabet.

7. Click **Save** to save the configuration file.

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

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

   The **Edit web server configuration file** pane opens on the right.

9. In the lower part of the opened pane, click the ✎ icon.

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

10. In the text editor window, enter the names of the certificate and key files that were uploaded in steps 3-4 to make sure that you uploaded the relevant certificate and key to the web server profile.

    ```
    ssl_certificate <certificate name>
    ```

    ```
    ssl_key <key name>
    ```

    > The current version of Kaspersky IoT Secure Gateway 1000 supports only the ssl_certificate and ssl_key settings of CivetWeb.

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

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

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

Modifying the web server profile

You can change the name and settings of the web server profile.

To change the web server profile name:

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

   The **Profiles** table is displayed.

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

   The **Edit web server profile** pane opens on the right.

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

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

The modified web server profile will appear in the **Profiles** table.

To change the settings of the web server profile:

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

   The **Profiles** table is displayed.

2. In the **Profiles** table, in the **Name** column, click the ⊞ icon next to the web server profile whose settings you want to change.

   This opens the **Profile settings** table containing a list of configuration files and certificates that are part of the web server profile. If the profile was created based on the **None** template, the list of files will be empty. An empty web server profile must be completed.

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

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

4. If you need to edit a configuration file, click the name of the configuration file and do the following in the **Edit web server configuration file** pane that opens on the right:

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

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

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

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

5. If you need to delete a configuration file, click the name of the configuration file and click the 🗑 icon located in the lower part of the **Edit web server configuration file** pane that opens on the right. Confirm file deletion.

   The selected configuration file will be deleted from the web server profile settings.

6. If you need to add a security certificate and key to the web server profile, do the following:

   a. Click the **Upload** button in the lower part of the page. In the opened file upload window, select a certificate file in PEM format with the CRT extension.

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

   b. Click the **Upload** button in the lower part of the page. In the opened file upload window, select a key file in PEM format with the KEY extension.

      The key file is uploaded to the system and appears in the profile settings.

7. If you need to remove a security certificate or key file from the profile, click the name of this certificate or key in the **Profile settings** table, click the 🗑 icon in the pane that opens on the right, and confirm its removal.

   The certificate or key file will be removed from the system.

Switching to a different web server profile

Kaspersky IoT Secure Gateway 1000 lets you switch between web server profiles. Different profiles enable you to work with different security certificates. The predefined web server profile is active by default.

To switch to a different web server profile:

1. In the menu in the left part of the web interface page, select **Settings** → **Web server**.
2. In the **Profiles** table, in the **Name** column, click the name of the web server profile that you want to set as active.

   The **Edit web server 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, next to the selected profile the icon ✓ will appear. The profile is now active and will be used for the Kaspersky IoT Secure Gateway 1000 web interface.

Deleting a web server profile

Kaspersky IoT Secure Gateway 1000 lets you delete web server profiles.

> Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined web server profile. If you need to delete the profile that is currently the active profile, you must first switch to a different web server profile.

To delete a web server profile:

1. In the menu in the left part of the web interface page, select **Settings** → **Web server**.
2. In the lower part of the window, in the **Profiles** table, in the **Name** column, click the name of the web server profile that you want to delete.

   The **Edit web server profile** pane opens on the right.
3. Click the 🗑 icon in the lower part of the pane and confirm profile deletion.

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

Configuring delivery of notifications when registering events

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

Configuring delivery of event logs to the Syslog server

Kaspersky IoT Secure Gateway 1000 can send network security event and audit logs to a Syslog server.

To configure forwarding of network security event and audit logs to a Syslog server:

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

   A page opens on the **Syslog** tab.
2. Set the **Use Syslog server to send events** toggle button to the enabled position.
3. Configure how event logs are forwarded by specifying the following settings:

- In the **IP address** field, enter the IP address and port of the recipient Syslog server like in the following example: `198.51.100.0:514`.

- In the **Mode** drop-down list, select the protocol that will be used by Kaspersky IoT Secure Gateway 1000 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 **Upload new certificate** button and select the relevant security certificate in the opened window.

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

Configuring delivery of push notifications

Firebase Cloud Messaging (FCM) is a cross-platform messaging solution that lets you reliably send messages for free.

Kaspersky IoT Secure Gateway 1000 uses Firebase Cloud Messaging 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 the provided topics of push notifications every four seconds to the topic /topics/DevicesandTopics residing in the FCM cloud service.

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

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"
}
```

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. For detailed information about creating an application to receive push notifications, please refer to the Firebase Cloud Messaging documentation ↗.

To configure the system name for sending push notifications:

1. In the menu in the left part of the web interface page, select **Settings** → **Utilities**.
2. Select the **Push notifications** tab.
3. In the **Device name** field, enter the name that will be used by the system to send push notifications.
4. In the **Authorization key** field, enter the Firebase authorization key.
5. If you need to upload a security certificate, click the **Upload new certificate** button and select the relevant security certificate in the opened window. Information about the uploaded certificate is displayed.

   > For push notifications to be sent correctly, make sure a valid security certificate has been downloaded.

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

Configuring delivery of MQTT notifications

Kaspersky IoT Secure Gateway 1000 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 **Settings** → **Utilities**.
2. Select the **MQTT notifications** tab.
3. Enable forwarding of MQTT notifications by setting the **Use MQTT to send events** toggle button to the enabled position.
4. Configure the settings for forwarding MQTT notifications:

   a. In the **IP address** field, enter the IP address of the MQTT broker you are using.

   b. In the **Port** field, enter the port number of the MQTT broker you are using.

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

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

   c. In the **MQTT topic name** field, specify the name of the MQTT-topic for sending notifications about audit events.

d. If you need to send notifications about audit events from a specific user, set the **Use authentication** toggle button to the enabled position and provide the following data:

   - In the **User name** field, enter the user login name for authorization on the server.
   - In the **Password** field, enter the password of the user login for authorization on the server.

     You can obtain the user account credentials from the system administrator. Sending notifications from a specific user is disabled by default.

e. If you need to use a secure SSL connection, set the **Use secure SSL connection** toggle button to the enabled position and do the following:

   1. Upload a certificate issued by a Certificate Authority. To do so, click the **Upload certificate** button and select a certificate file on the local device.

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

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

   2. Upload the client certificate. To do so, click the **Upload client certificate** button and select a certificate file on the local device.

      Information about the uploaded client certificate will be displayed on the page.

   3. Upload a key for the client certificate. To do so, click the **Upload key** button and select a key file on the local device.

   Use of a secure SSL connection is disabled by default.

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

Configuring the date and time

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

To configure the date and time:

1. In the menu in the left part of the web interface page, select **Settings** → **General** → **Date and time**.
2. Specify the current date in the **Day**, **Month** and **Year** drop-down lists.
3. Click **Save** in the date editing block to save the changes.
4. Specify the current time in the **Hours**, **Minutes**, and **Seconds** drop-down lists.

   > Indicate the current time in the UTC+00:00 time zone.

5. Click **Save** in the time editing block to save the changes.

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

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

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

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

   The user menu appears.

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

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

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

Performing common tasks

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

Monitoring the state of Kaspersky IoT Secure Gateway 1000

Summary information about the state of Kaspersky IoT Secure Gateway 1000 and the network security state is displayed in the **Dashboard** section of the web interface. This section contains the following information blocks:

- **Information**. Contains the name and serial number of the hardware platform, and the Kaspersky IoT Secure Gateway 1000 application version.
- **Events**. Contains information about the number of network security events for each entity that registered events.

  > Network security events are not stored in the system and are available only while the current session of the connection to the Kaspersky IoT Secure Gateway 1000 web interface is active.

- **Audit**. Contains information on Kaspersky IoT Secure Gateway 1000 security-related events that were written to the audit log. The following system security statuses are available:
  - **Issues** – events with *Warning* or *Critical* severity were registered.
  - **No errors** – there are no events or there are only events with *Informational* severity.
- **MQTT broker**. Contains information about Kaspersky IoT Secure Gateway 1000 operation statistics over the MQTT protocol and information about issues with data transfer via MQTT:
  - **Issues** – issues with data transfer over the MQTT protocol were detected.
  - **No errors** – there are no issues.
- **Devices**. Contains information about the number of devices detected in the network.

You can view detailed information in each information block by clicking **Show** in the right part of the block.

Monitoring the state of a cellular connection

> If a device does not have a modem, the use of a cellular connection and configuration of cellular connection settings are unavailable.

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

- **Modem status** – displays the state of the Kaspersky IoT Secure Gateway 1000 cellular connection. The following values are available for this setting:
  - A gray icon means that the modem is currently not available for use.

  - A green icon means that the modem is connected to the cellular network provider.

    If you want to use the modem as the main communication channel, you need to enable the use of a cellular connection for Kaspersky IoT Secure Gateway 1000.

  - A red icon means that there is no connection between the modem and the cellular network provider.

- **Signal quality** – displays the quality of the cellular connection between Kaspersky IoT Secure Gateway 1000 and the external network.

  The number of lines denotes the signal quality of the cellular communication network that the device is connected to. As the signal quality decreases, the number of bars is reduced.

In the **Modem DNS server addresses** block, you can view information about the IP addresses of the primary and secondary DNS servers of the modem.

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

- The SIM card used in the modem is valid and has an active plan that supports an Internet connection through the modem.

- The selected modem profile matches the utilized SIM card.

- The modem is available for use (a green icon is displayed in the **Modem settings** block).

  If the modem is not available for use (a gray or red icon is displayed in the **Modem settings** block), you must restart Kaspersky IoT Secure Gateway 1000 and re-check whether the modem is available for use after the restart. Devices that access the Internet through Kaspersky IoT Secure Gateway 1000 must obtain the internal network settings through the DHCP server of Kaspersky IoT Secure Gateway 1000. The relevant addresses of DNS servers from cellular network providers will be received together with these settings.

Monitoring devices in Kaspersky IoT Secure Gateway 1000

This section contains instructions on monitoring devices in Kaspersky IoT Secure Gateway 1000 and managing the list of allowed devices.

Viewing the list of devices

The **Devices** section displays information about devices that Kaspersky IoT Secure Gateway 1000 detected in the network.

Kaspersky IoT Secure Gateway 1000 divides detected devices into authorized devices and unauthorized devices. Each new device detected in the network by the system is considered to be an unauthorized device. To make a device authorized, you need to add it to the allowlist.

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

To view the list of devices detected by Kaspersky IoT Secure Gateway 1000:

1. In the left part of the page in the menu of the Kaspersky IoT Secure Gateway 1000 web interface, select the **Devices** section.

This opens the **Devices** page that shows a table of devices detected in the network.

> The table displays the devices detected by the system when the **Devices** section is opened. The device table is not updated automatically. By default, the table displays all unauthorized devices of all the detected types.

> When devices are detected in the enterprise network, the device name may contain personal data of the user. You need to rename a device when adding it to the allowlist.

> If an authorized device disappears from the network for a period of three minutes, its IP address information will be removed from the table of detected devices. When the device is detected again on the network, its IP address is updated. If an unauthorized device disappears from the network for a period of three minutes, it is automatically deleted from the table of detected devices.

The following information is displayed for each device detected by the system:

- **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.
- **Info** – additional information that could be identified for the device, such as the operating system and device vendor.

2. If you need to sort devices in the table, click the header of the relevant column. For example, to sort devices by type, click the header of the **Type** column.
3. If you need to refresh the list of detected devices, click the **Update** button in the upper part of the page.
4. If you need to filter the list of displayed devices based on the device type, click the button containing the name of the device type in the **Type** block above the table.

   Devices of the selected type will no longer be displayed in the **Devices** table, and the button with the device type will no longer be highlighted. If you need to enable display of devices, click the button containing the name of this device type again (the button will be highlighted in blue again).
5. If you need to display only devices that are on the list of allowed devices, set the **Allowlist** toggle button to the enabled position.

Adding and removing devices from the list of allowed devices

Kaspersky IoT Secure Gateway 1000 divides detected devices into authorized devices and unauthorized devices. Each new device detected in the network by the system is considered to be an unauthorized device. To make a device authorized, you need to add it to the list of allowed devices.

In the **Devices** section, you can add devices to the allowlist or remove devices from this list.

To add or remove a device from the allowlist:

1. In the **Devices** section, select the check box next to the name of the device that you want to add or remove from the allowlist.
2. In the pane that opens on the right, do one of the following:
   - If you need to add the device to the authorized list, click the **Add to device allowlist** button.

     The pane containing the device icon closes. The device will appear in the allowlist, and the status of the device will change to *Authorized*.
   - If you need to remove the device from the authorized list, click the **Remove from device allowlist** button.

     The pane on the right closes. The device will disappear from the allowlist, and the status of the device will change to *Unauthorized*.

Monitoring events of Kaspersky IoT Secure Gateway 1000

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

About Kaspersky IoT Secure Gateway 1000 events

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

Kaspersky IoT Secure Gateway 1000 registers the following events related to network security:

- *Attack detected* – this event is registered when an attack is detected and/or blocked (depending on the IPS settings).
- *Unknown Device* – this event is registered when an untrusted device is connected to the network.
- *Device removed* – this event is registered when a device is removed from the network.

Network security events are distinguished based on the following severity levels:

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

Kaspersky IoT Secure Gateway 1000 registers the following events related to the security of Kaspersky IoT Secure Gateway 1000:

- *All secure entities started and running*. All entities of Kaspersky IoT Secure Gateway 1000 are running in normal mode.

- *Internal error*. An internal error occurred in Kaspersky IoT Secure Gateway 1000.

- *Partition reverted*. Kaspersky IoT Secure Gateway 1000 entity was recovered.

- *Update committed*. Kaspersky IoT Secure Gateway 1000 was updated.

- *Update requested*. An update was requested for Kaspersky IoT Secure Gateway 1000.

- *Unable to start device detector*. An attempt to start monitoring devices on the network failed.

- *Unable to restart device detector*. A repeated attempt to start monitoring devices on the network failed.

- *FW: Firewall config is changed*. Firewall settings were modified.

- *Package verification problem*. An update package for Kaspersky IoT Secure Gateway 1000 could not be verified.

- *An error occurred while unpacking or deploying package*. An error occurred while unpacking or deploying a Kaspersky IoT Secure Gateway 1000 update package.

- *An error occurred while applying package*. An error occurred during installation of the Kaspersky IoT Secure Gateway 1000 update package.

- *UBOOT: Update image authentication failed!* An error occurred when verifying the Kaspersky IoT Secure Gateway 1000 image.

- *UBOOT: Failed to cancel update!* An error occurred when canceling an update of Kaspersky IoT Secure Gateway 1000.

- *UBOOT: Image authentication failed, reverting!* An error occurred when verifying the Kaspersky IoT Secure Gateway 1000 image during an update rollback.

- *UBOOT: Failed to revert!* An error occurred during an update rollback.

- *UBOOT: No update image found!* A Kaspersky IoT Secure Gateway 1000 image was not found.

- *UBOOT: No image found, reverting!* An image was not found for Kaspersky IoT Secure Gateway 1000, so it was rolled back to the previous version.

- *UBOOT: Failed to set update flag while loading*. The update flag could not be set when loading the Kaspersky IoT Secure Gateway 1000 image.

About Kaspersky IoT Secure Gateway 1000 logs

Kaspersky IoT Secure Gateway 1000 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 1000, such as the component security status after the application is loaded.

Kaspersky IoT Secure Gateway 1000 lets you view network security-related events and audit events through the web interface, and forward them to a recipient Syslog server. If necessary, you can also configure forwarding of push notifications and MQTT notifications about registered events.

Viewing the network security log

Kaspersky IoT Secure Gateway 1000 lets you view network security events that occur during the current session of the user's connection to the system through a browser.

To view network security events:

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

   This opens the **Network security events** page, which provides a table of log entries for network security events. The following information is displayed for each table entry:

   - **Entity** – name of the architectural component of Kaspersky IoT Secure Gateway 1000 that registered the particular event. For example, *Traffic processor*.
   - **Event** – type of event.
   - **Title**: information about the registered network security event (such as the detection of an unknown device or blocked attack).
   - **Date and time** – date and time when the network security event was registered.

2. If you need to sort events in the table, click the header of the relevant column. For example, click the **Entity** column to sort by component name.

3. If you need to enable automatic updates of event log entries on the page, set the **Auto-update** toggle button to the enabled position.

   If the **Auto-update** toggle button is switched off, the page displays only those events that were in the log when the **Network security events** section was opened. **Auto-update** is disabled by default.

4. If you need to filter the list of events that were registered by a specific entity, click the button containing the entity name above the table.

   Events that were registered by this entity will no longer be displayed in the **Network security events** table, and the button containing the entity name will no longer be highlighted. If you need to enable display of events, click the button containing the name of the relevant entity again (the button will be highlighted in blue again).

Viewing the audit log

Kaspersky IoT Secure Gateway 1000 saves events related to system security in the audit log.

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

> Exporting an audit log on the local computer will result in deletion of the audit log from the system.

To view the audit log:

1. 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. The following information is displayed for each audit log entry:

   - 🔥 – severity of the event.
   - **Title** – detailed information about the registered event, such as modified firewall settings.
   - **Entity** – name of the architectural component of Kaspersky IoT Secure Gateway 1000 that registered the particular event.
   - **Date and time** – date and time when the event was registered.

2. If you want the table to hide events that have a specific severity level, click the icon of the relevant severity level icon above the table.

   Events with this severity level will be hidden in the **System security audit** table, and the button containing the severity level icon will no longer be highlighted. If you need the table to display events that were hidden, click the button containing the icon of the relevant severity level (the button will be highlighted in blue again).

3. If you need to hide events that were registered by a specific entity, click the button containing the entity name above the table.

   Events that were registered by this entity will be hidden in the **System security audit** table, and the button containing the entity name will no longer be highlighted. If you need the table to display events that were filtered out of the display, click the button containing the name of the relevant entity again (the button will be highlighted in blue again).

4. If you need to select a specific period for displaying events, select one of the following values in the **Period** drop-down list:

   - **All periods**.
   - **Last day**.
   - **Last week**.
   - **Last month**.

5. If you need to sort events in the table, click the header of the relevant column. For example, to sort events by description, click on the header of the **Title** column.

6. If you need to enable automatic updates of event log entries on the page, set the **Auto-update** toggle button to the enabled position.

   If **Auto-update** is disabled, the page displays only those events that were in the audit log when the **Audit** section was opened. **Auto-update** is disabled by default.

   If you need to view information about audit log settings, in the **System security audit** section, move your mouse cursor over the ⓘ icon in the upper part of the window.

   This opens a window containing the following information:

   - **Total entries** – current number of entries in the audit log.
   - **Maximum** – maximum number of entries in the audit log.
   - **Policy** – audit log entry maintenance policy:

- *Cyclical* – when the audit log is overfilled, new entries will overwrite old entries.
- *Limited* – when the audit log is overfilled, the system stops.

Audit log settings are configured by Kaspersky experts when building Kaspersky IoT Secure Gateway 1000 and cannot be changed through the Kaspersky IoT Secure Gateway 1000 web interface.

Exporting the audit log

You can save the Kaspersky IoT Secure Gateway 1000 audit log on the local computer.

To save the audit log on the local computer:

1. In the **System security audit** section, click the **Save to file** button.

   This opens a window warning you that the audit log will be deleted from Kaspersky IoT Secure Gateway 1000 after you save the file.

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

   This opens a window that lets you save the audit log to a file.

3. In the opened window, specify the path for saving the audit log file on the local computer and save the file.

The Kaspersky IoT Secure Gateway 1000 audit log will be saved on the local computer. By default, the file is saved with the name audit.csv.

Exporting event logs of Kaspersky IoT Secure Gateway 1000

You can export information about Kaspersky IoT Secure Gateway 1000 events to a GZIP file. This archive contains log files that include network security events, audit events, and diagnostic information. These files can be used for analysis of the audit and network security of Kaspersky IoT Secure Gateway 1000, and for diagnostics of potential system issues.

To save Kaspersky IoT Secure Gateway 1000 event logs on the local computer:

1. In the menu in the left part of the web interface page, select **Settings** → **General** → **Event information**.

2. Click the **Save to file** button and save the archive on the local computer.

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

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

Kaspersky IoT Secure Gateway 1000 lets you view Kaspersky IoT Secure Gateway 1000 event logs in real time. To do this, you need to connect Advantech UTX-3117FS-S6A1N to a local computer via console port.

A *console port* is a control port providing out-of-band access to the Advantech UTX-3117FS-S6A1N device.

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

1. Please connect a null-modem crossover cable (DB-9f/DB-9f) to the Advantech UTX-3117FS-S6A1N rear panel at one end and to a desktop or laptop computer at the other.

   If your computer does not have a null-modem crossover cable connector, you can use a USB-COM adapter.

2. Turn on the Advantech UTX-3117FS-S6A1N.

3. Using a terminal emulator on a local computer, connect to Advantech UTX-3117FS-S6A1N.

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

   - The data transfer rate should be 115,200 baud, or a different value if it is specifically set for the **Recovery mode** parameter

   - The number of data bits, availability and type of the parity bit, and the number of stop bits should be 8n1

   - Hardware flow control

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

Managing the application through the Kaspersky Security Center 13.2 Web Console

The Kaspersky Security Center 13.2 Web Console (hereinafter also referred to as simply "the Web Console") is a web application designed to let you centrally perform the main tasks for managing and maintaining the security system of an enterprise network. The Web Console is a Kaspersky Security Center 13.2 component that provides a user interface. For detailed information about the Kaspersky Security Center 13.2 Web Console, please refer to the Kaspersky Security Center 13.2 Online Help Guide.

> Kaspersky Security Center 13.2 and Kaspersky Security Center 13.2 Web Console are not included in the Kaspersky IoT Secure Gateway 1000 distribution kit. They must be installed separately.

You can use the Kaspersky Security Center 13.2 Web Console to do the following:

- Monitor the state of your organization's security system.
- Manage installed applications.
- View reports on the security system state.

> Information about Kaspersky IoT Secure Gateway 1000 may not be displayed, when you view information about a device with Kaspersky IoT Secure Gateway 1000 in the Web Console on the **General** tab in the **General**, **Network**, **System**, **Protection**, **Device status determined by application** sections.

Kaspersky IoT Secure Gateway 1000 is synchronized with Kaspersky Security Center every 30 seconds, which is known as the "heartbeat" interval. At this interval, the Kaspersky Security Center 13.2 Web Console receives information about network security events registered in Kaspersky IoT Secure Gateway 1000, and any settings that are defined in the Kaspersky IoT Secure Gateway 1000 interface or in the Web Console are synchronized. Kaspersky IoT Secure Gateway 1000 network security events include the detection of devices in the network, and any attempts to connect to the Kaspersky IoT Secure Gateway 1000 web interface.

About the Kaspersky IoT Secure Gateway 1000 administration web plug-in

The Kaspersky IoT Secure Gateway 1000 administration web plug-in (hereinafter also referred to as simply "the web plug-in") facilitates interaction between Kaspersky IoT Secure Gateway 1000 and the Kaspersky Security Center 13.2 Web Console.

The web plug-in lets you centrally perform the following actions through the Kaspersky Security Center 13.2 Web Console:

- Configure the settings of Kaspersky IoT Secure Gateway 1000.
- Receive events from Kaspersky IoT Secure Gateway 1000.
- Manage the firewall.
- Manage the Intrusion Prevention system.
- Manage the security of Kaspersky IoT Secure Gateway 1000.

- Restart and update Kaspersky IoT Secure Gateway 1000.

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

The Kaspersky IoT Secure Gateway 1000 administration web plug-in is not installed in the Kaspersky Security Center 13.2 Web Console by default. The Kaspersky IoT Secure Gateway 1000 administration web plug-in is included in the Kaspersky IoT Secure Gateway 1000 distribution kit. You must install the web plug-in on the computer that has the Kaspersky Security Center 13.2 Web Console installed. The web plug-in functionality is available to all administrators that can access the Kaspersky Security Center 13.2 Web Console in a browser. The list of installed web plug-ins is displayed in the Kaspersky Security Center 13.2 Web Console interface (**Console settings** → **Web plug-ins**).

> Port 13294 must be accessible on the Administration Server where Kaspersky Security Center is installed. Port 13294 is required for connecting UEFI protection devices. For more details about managing UEFI protection devices, please refer to the *UEFI protection devices* section in the Kaspersky Security Center 13.2 Online Help Guide. For more details about the ports used for connecting to Kaspersky Security Center, please refer to the section titled *Ports used by Kaspersky Security Center* in the Kaspersky Security Center 13.2 Online Help Guide.

> Kaspersky Security Center 13.2 and Kaspersky Security Center 13.2 Web Console are not included in the Kaspersky IoT Secure Gateway 1000 distribution kit. They must be installed separately.

To install the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 13.2 Web Console:

1. In the menu of the Kaspersky Security Center 13.2 Web Console, select **Console settings** → **Web plug-ins**.

   A list of available administration plug-ins for the Kaspersky Security Center 13.2 Web Console will appear.

2. Click the **Add from file** button.

3. In the opened pane on the right, add the following files:

   - ZIP archive containing the web plug-in distribution package received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download ZIP file** button.

   - Signature file received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download signature** button.

4. Click the **Add** button.

5. When installation of the web plug-in is complete, click **OK**.

The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be downloaded to the default configuration and will appear in the list of Kaspersky Security Center 13.2 administration plug-ins.

Updating the Kaspersky IoT Secure Gateway 1000 administration web plug-in

You can update the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 13.2 Web Console.

To update the Kaspersky IoT Secure Gateway 1000 administration web plug-in in the Kaspersky Security Center 13.2 Web Console:

1. In the menu of the Kaspersky Security Center 13.2 Web Console, select **Console settings → Web plug-ins**.

   A list of available administration plug-ins for the Kaspersky Security Center 13.2 Web Console will appear.

2. In the list of administration plug-ins, select the check box next to the Kaspersky IoT Secure Gateway 1000 administration web plug-in.

3. Click the **Update from file** button.

4. In the opened pane on the right, add the following files:

   - ZIP archive containing the web plug-in distribution package received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download ZIP file** button.

   - Signature file received in the Kaspersky IoT Secure Gateway 1000 distribution kit by clicking the **Download signature** button.

5. Click **Update**.

6. When the update is complete, click **OK**.

The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be updated, and its version information and update time will be displayed in the table of administration web plug-ins in the Kaspersky Security Center 13.2 Web Console.

Removing the Kaspersky IoT Secure Gateway 1000 administration web plug-in

The Kaspersky IoT Secure Gateway 1000 administration web plug-in can be removed in the Kaspersky Security Center 13.2 Web Console. After the web plug-in is removed, you will not be able to manage Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

To remove the Kaspersky IoT Secure Gateway 1000 administration web plug-in from the Kaspersky Security Center 13.2 Web Console:

1. In the web interface menu of the Kaspersky Security Center 13.2 Web Console, select **Console settings → Web plug-ins**.

   A list of available administration plug-ins for the Kaspersky Security Center 13.2 Web Console will appear.

2. In the list of administration plug-ins, select the check box next to the Kaspersky IoT Secure Gateway 1000 administration web plug-in.

3. Click the **Delete** button.

4. In the plug-in removal confirmation window that opens, do one of the following:

   - If you need to save a backup copy of the plug-in, click **OK**.

     A backup copy of the plug-in will be created. The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be removed from the Kaspersky Security Center 13.2 Web Console.

- If you do not need to save a backup copy of the plug-in, click the **Skip data backup** button.

  The Kaspersky IoT Secure Gateway 1000 administration web plug-in will be removed from the Kaspersky Security Center 13.2 Web Console.

5. In the opened window containing information about plug-in removal, click **OK**.

Logging into and logging out of the Kaspersky Security Center 13.2 Web Console

To log in to the Kaspersky Security Center 13.2 Web Console, you need to ask the administrator for the web address of the Kaspersky Security Center Administration Server and the port number that was specified during installation (port 8080 is used by default). You must also enable JavaScript in your browser.

To log in to the Kaspersky Security Center 13.2 Web Console:

1. In your browser, open `https://<address>:<port>`.

   For the requirements of the browser used to work with the Kaspersky Security Center 13.2 Web Console, please refer to the *Hardware and software requirements* section of the *Kaspersky Security Center 13.2 Online Help Guide*.

   The login page opens.

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

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

   After logging in, the Dashboard appears displaying the last language and theme that were used.

   If you are logging in to the Kaspersky Security Center 13.2 Web Console for the first time, a tutorial is displayed in the lower part of the screen. You can follow the instructions of the tutorial, or close it.

You are now logged in Kaspersky Security Center 13.2 Web Console and can work with the Kaspersky Security Center 13.2 Web Console. For additional information about how the Kaspersky Security Center 13.2 Web Console works, please refer to the Online Help Guide for Kaspersky Security Center 13.2.

To log out of the Kaspersky Security Center 13.2 Web Console:

1. In the menu of the Kaspersky Security Center 13.2 Web Console, click the user name.

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

The Kaspersky Security Center 13.2 Web Console closes and the login page is displayed.

Adding a Kaspersky IoT Secure Gateway 1000 device to the group of managed devices of the Kaspersky Security Center 13.2 Web Console

To use the Kaspersky Security Center 13.2 Web Console to manage a device with Kaspersky IoT Secure Gateway 1000 installed, move this device to the group of managed devices.

To add a device to the group of managed devices in the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Kaspersky Security Center 13.2 Web Console, select **Device discovery and deployment** → **Unassigned devices**.

   The list of all detected unassigned devices will be displayed.

2. Select the check box next to the name of the device that you want to add to the group of managed devices.

3. Click the **Move to group** button.

   The **Move to group** pane opens on the right.

4. Select the check box next to the **Managed devices** administration group.

5. Click the **Move** button.

The device will be moved to the managed devices group.

Configuring Kaspersky IoT Secure Gateway 1000 settings through the Kaspersky Security Center 13.2 Web Console

This section contains information about configuring Kaspersky IoT Secure Gateway 1000 settings through the Kaspersky Security Center 13.2 Web Console.

Configuring network settings through the Kaspersky Security Center 13.2 Web Console

The Kaspersky IoT Secure Gateway 1000 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. You can also configure the network settings by using the web interface of Kaspersky IoT Secure Gateway 1000.

To configure network settings through the Kaspersky Security Center 13.2 Web Console:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Network** → **LAN** and configure the following settings:

   a. In the **IP address** field, enter the IP address of the Kaspersky IoT Secure Gateway 1000 device in the internal network.

   b. In the **Subnet mask** field, enter the subnet mask.

c. If you need Kaspersky IoT Secure Gateway 1000 to act as a DHCP server, set the toggle button to **Use DHCP server** and specify the following settings:

   - In the **Start of IP address range** field, enter the starting IP address of the range.
   - In the **End of IP address range** field, enter the ending IP address of the range.
   - In the **Primary DNS server** 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.

7. Click the **Save** button.
8. In the **Network** section, select the **WAN** tab and configure the following settings:

   - If you want to configure WAN settings automatically using the DHCP protocol, set the toggle button to **DHCP client is enabled**.

     > If the DHCP server issued null DNS server addresses to Kaspersky IoT Secure Gateway 1000 when enabling automatic configuration of external network settings, the IP address 208.67.222.222 (OpenDNS server) will be used by default to convert a domain name to an IP address.

   - If you want to manually configure the WAN settings, set the toggle button to **DHCP client is disabled** and do the following:

     - In the **IP address** field, enter the IP address that you want to assign to the system in the external network.
     - In the **Subnet mask** field, enter the subnet mask.
     - In the **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.

9. Click the **Save** button.

Configuring Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Kaspersky Security Center 13.2 Web Console

You can view and configure the Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Kaspersky Security Center 13.2 Web Console.

If the device does not have a modem, you cannot use a cellular connection in Kaspersky IoT Secure Gateway 1000 and cannot configure the Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Kaspersky Security Center 13.2 Web Console.

To view the Kaspersky IoT Secure Gateway 1000 cellular connection settings through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.

   A window displaying the following information about the cellular connection of Kaspersky IoT Secure Gateway 1000 will appear:

   - The **Modem settings** block provides information about the modem operating status and current signal quality.
   - The **Modem DNS server addresses** block provides information about the IP addresses of the primary and secondary DNS servers of the modem.
   - The **Modem profiles** table displays information about the available modem profiles.

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

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

Different modem profiles enable you to work with different cellular communication providers. To use a cellular connection, one of the modem profiles must be active. The predefined modem profile is active by default.

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

- The SIM card used in the modem is valid and has an active plan that supports an Internet connection through the modem.
- The selected modem profile matches the utilized SIM card.
- The modem is available for use (a green icon is displayed in the **Modem settings** block).

  If the modem is not available for use (a gray or red icon is displayed in the **Modem settings** block), you must restart Kaspersky IoT Secure Gateway 1000 and re-check whether the modem is available for use after the restart. Devices that access the Internet through Kaspersky IoT Secure Gateway 1000 must obtain the internal network settings through the DHCP server of Kaspersky IoT Secure Gateway 1000. The relevant addresses of DNS servers from cellular network providers will be received together with these settings.

Enabling and disabling the Kaspersky IoT Secure Gateway 1000 cellular connection through the Kaspersky Security Center 13.2 Web Console

Kaspersky IoT Secure Gateway 1000 processes outgoing and incoming network traffic using a cellular connection (through a cellular communications provider). You can enable or disable use of a Kaspersky IoT Secure Gateway 1000 cellular connection through the Kaspersky Security Center 13.2 Web Console. Use of a cellular connection is disabled by default.

To enable or disable the use of a cellular connection for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.
7. In the **Modem settings** block, move the toggle button to **Use modem as main communication channel** to enable use of the cellular connection, or move it to **Do not use modem as main communication channel** to disable use of the cellular connection.

The Kaspersky IoT Secure Gateway 1000 cellular connection will be enabled or disabled according to your selection.

Creating a modem profile for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console

You can create new modem profiles for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console. Different modem profiles enable you to work with different cellular communication providers.

To create a new modem profile for Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Network** → **Modem**.

7. In the **Modem profiles** table, click the **Add** button.

   The pane for adding a modem profile opens on the right.

8. In the **Status** drop-down list, select the profile status. The following values are available:

   - **Active**. The selected modem profile will be used as the main modem profile for the cellular connection of Kaspersky IoT Secure Gateway 1000. The ✓ icon appears next to the active profile in the **Active** column of the **Profiles** table.

   - **Inactive**.

9. In the **Profile name** field, enter the profile name.

10. In the **Configuration file** field, enter the modem profile configuration settings.

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

    The pane for adding a modem profile will close. The new profile will be displayed in the **Modem profiles** table.

12. Click **Save** in the lower part of the modem settings window to save the changes.

Editing the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console

You can change the settings of the Kaspersky IoT Secure Gateway 1000 modem profile through the Kaspersky Security Center 13.2 Web Console.

To change the settings of the Kaspersky IoT Secure Gateway 1000 modem profile through the Kaspersky Security Center 13.2 Web Console:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Network** → **Modem**.

7. In the **Modem profiles** table, select the check box next to the modem profile that you need to edit and click the **Edit** button in the upper part of the table.

8. In the modem profile editing pane that opens on the right:

a. Select one of the following values from the **Status** drop-down list if you need to change the status of a profile:

- **Active**. After saving the changes, the selected modem profile will be used as the main modem profile for the cellular connection of Kaspersky IoT Secure Gateway 1000. The ✓ icon appears next to the active profile in the **Active** column of the **Profiles** table.

- **Inactive**.

> When the modem profile status is changed to **Active**, you must restart Kaspersky IoT Secure Gateway 1000 for this change to take effect.

b. If necessary, enter a new profile name in the **Profile name** field.

c. You can edit the current settings or enter new settings for the modem profile in the **Configuration file** field.

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

The pane for editing the modem profile will close. The modified profile will be displayed in the **Modem profiles** table.

9. Click **Save** in the lower part of the modem settings window to save the changes.

Deleting the modem profile of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console

You can delete a modem profile through the Kaspersky Security Center 13.2 Web Console.

> Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined modem profile. If you need to delete the profile that is currently the active profile, you must first select a different modem profile as active.

To delete a Kaspersky IoT Secure Gateway 1000 profile through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Modem**.
7. In the **Modem profiles** table, select the check box next to the modem profile that you need to delete and click the **Delete** button.

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

8. Click **Save** in the lower part of the modem settings window to save the changes.

The selected modem profile will be deleted.

Managing certificates through the Kaspersky Security Center 13.2 Web Console

You can view previously uploaded certificates and update certificates via the Kaspersky Security Center 13.2 Web Console.

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

To add or delete certificates in Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Certificate**.

   This opens a window displaying the following information about certificates:

   - The **Administrator certificate** area shows data on the current administrator certificate.
   - The **Kaspersky Security Center server certificate** area shows data on the current certificate of the Kaspersky Security Center server.
7. If you need to add a new administrator certificate, click the **Upload** button in the **Administrator certificate** block and select the certificate file in the window that opens. Only files in CRT, PEM, DER, or CER format can be added as a certificate.

   The new administrator certificate will upload to the system and the previously uploaded certificate will be deleted.

   > Kaspersky IoT Secure Gateway 1000 does not let you delete an administrator certificate without replacing the certificate with a new one.
8. Click **Save** in the lower part of the window to save the changes.

If a new certificate was issued for the Kaspersky Security Center Administration Server, the connection that was previously established between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center will be terminated. To resume the connection, you will need to add the newly issued certificate as a Kaspersky Security Center server certificate in the Kaspersky IoT Secure Gateway 1000 web interface.

Viewing the list of web server profiles through the Kaspersky Security Center 13.2 Web Console

Operation of the Kaspersky IoT Secure Gateway 1000 web interface is supported by a web server. Web server settings are stored in a web server profile. Using the Kaspersky Security Center 13.2 Web Console, you can only view existing web server profiles. Web server profiles can be managed through the Kaspersky IoT Secure Gateway 1000 web interface.

To view the list of web server profiles:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Web server**.

   This opens a table of web server profiles showing the following information for each web server profile:

   - 🔒 – web server profile editing access. This icon indicates that a profile is read-only and is only displayed for predefined profiles.
   - **Active** – the ✓ icon indicates that the web server profile is currently being used in the application.
   - **Name** – name of the web server profile.
   - **Modified** – date and time of the most recent change in the profile.

Configuring MQTT broker settings through the Kaspersky Security Center 13.2 Web Console

In the Kaspersky Security Center 13.2 Web Console, you can create new MQTT broker profiles, edit existing profiles, and switch between profiles.

This section contains information about configuring MQTT broker settings through the Kaspersky Security Center 13.2 Web Console.

Creating an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console

You can create new MQTT broker profiles through the Kaspersky Security Center 13.2 Web Console. Different MQTT broker profiles let you work with different servers and digital platforms that receive events from Kaspersky IoT Secure Gateway 1000 over the MQTT protocol.

To create a new MQTT broker profile through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT** section.

   The table of MQTT broker profiles is displayed.
7. Click the **Add** button in the upper part of the MQTT broker profiles table.

   The **Edit profile** window opens.
8. In the **Status** drop-down list, select one of the following values:
   - **Active**, if you want to make a new profile active. In this case, profile settings are uploaded to the MQTT broker and access to certificates from the profile is activated for the MQTT broker.
   - **Inactive**.

   > Only one profile can be active.
9. In the **Name** field, enter the profile name using letters of the English alphabet.
10. Add a configuration file or certificate to the new profile by clicking the **Add** button in the upper part of the **List of files** table.
11. In the file upload pane that opens on the right, do the following:

    a. In the **Type** drop-down list, select the type of file that you want to add:
       - **Main configuration file**. This contains the main settings for MQTT broker operation. The main configuration file must be added to the MQTT broker profile so that this profile can be activated. Files in CONF format can be selected.
       - **Configuration file**. This contains additional settings for MQTT broker operation. Files in CONF format can be selected.

- **Certificate**. If you are planning to use an MQTT broker profile to connect to devices or cloud services in an external network, you must upload the Certification Authority certificate, client certificate, and private key. In Kaspersky IoT Secure Gateway 1000, you can only upload certificates in PEM format with the CRT extension, and keys in PEM format with the KEY extension.
- **Other**. Contains additional information for MQTT broker operation. Any type of file can be selected.

b. Click the **Upload file** button and select a file in the opened file upload window. The file size must not exceed 131 KB.

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

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

The file upload pane closes.

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

    The **Edit profile** window closes.

13. Click **Save** in the lower part of the window to save the new MQTT broker profile.

Editing an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console

You can change the settings of an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console.

To change an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT** section.

   The table of MQTT broker profiles is displayed.
7. In the table of MQTT broker profiles, select the profile that you want to edit and click the **Edit** button in the upper part of the table.

   The **Edit profile** window opens.
8. In the **Status** drop-down list, select **Active** if you want to make this profile active. In this case, profile settings are uploaded to the MQTT broker and access to certificates from the profile is activated for the broker.

   > Only one profile can be active.

9. If you need to change the profile name, enter the profile name using letters of the English alphabet in the **Name** field.

   For a profile provided together with the device (predefined profile), the **Name** field cannot be edited.

10. If you want to add a configuration file or certificate to the profile, click the **Add** button in the upper part of the **List of files** table.

    The file upload pane opens on the right.

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

    - **Main configuration file**. This contains the main settings for MQTT broker operation. The main configuration file must be added to the MQTT broker profile so that this profile can be activated. Files in CONF format can be selected.
    - **Configuration file**. This contains additional settings for MQTT broker operation. Files in CONF format can be selected.
    - **Certificate**. If you are planning to use an MQTT broker profile to connect to devices or cloud services in an external network, you must upload the Certification Authority certificate, client certificate, and private key. In Kaspersky IoT Secure Gateway 1000, you can only upload certificates in PEM format with the CRT extension, and keys in PEM format with the KEY extension.
    - **Other**. Contains additional information for MQTT broker operation. Any type of file can be selected.

    b. Click the **Upload file** button and select a file in the opened file upload window. The file size must not exceed 131 KB.

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

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

    The file upload pane closes. The file will be added to the MQTT broker profile and will appear in the **List of files** table.

11. If you want to delete a previously added configuration file or certificate in the MQTT broker profile, select the file that you want to delete and click the **Delete** button in the upper part of the **List of files** table.

    The file will be deleted from the MQTT broker profile.

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

    The **Edit profile** window closes.

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

Deleting an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console

You can delete MQTT broker profiles through the Kaspersky Security Center 13.2 Web Console.

> Kaspersky IoT Secure Gateway 1000 does not let you delete the active or predefined MQTT broker profile. If you need to delete the profile that is currently the active profile, you must first select a different MQTT broker profile as active.

To delete an MQTT broker profile through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select the **MQTT** section.
7. In the table of MQTT broker profiles, select the profile that you want to delete and click the **Delete** button in the upper part of the table.
8. Click **Save** in the lower part of the window to save the changes.

The selected MQTT broker profile will be deleted.

Configuring notifications through the Kaspersky Security Center 13.2 Web Console

This section contains information about configuring notifications through the Kaspersky Security Center 13.2 Web Console for registration of events in the system.

Configuring push notifications to a Syslog server through the Kaspersky Security Center 13.2 Web Console

Kaspersky IoT Secure Gateway 1000 includes a Syslog client that you can use to send notifications about audit and security events to a Syslog server. You can configure forwarding of notifications to a Syslog server through the Kaspersky Security Center 13.2 Web Console.

To configure delivery of notifications to a Syslog server:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.

6. Select **Notifications** → **Syslog**.

7. Set the toggle button in the upper part of the window to **Use Syslog server** and specify the following settings:

   - In the **IP address** field, specify the IP address of the Syslog server.

   - In the **Port** field, specify the port that will be used for the connection.

   - In the **Mode** drop-down list, select one of the following connection options:

     - **UDP**.

     - **TCP**.

     - **TLS**.

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

Kaspersky IoT Secure Gateway 1000 can send notifications about security events and audit events to a Syslog server.

Configuring delivery of push notifications through the Kaspersky Security Center 13.2 Web Console

Firebase Cloud Messaging (FCM) is a cross-platform messaging solution that lets you reliably send messages for free.

Kaspersky IoT Secure Gateway 1000 uses Firebase Cloud Messaging ↗ 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 the provided topics of push notifications every four seconds to the topic /topics/DevicesandTopics residing in the FCM cloud service. You can configure delivery of push notifications through the Kaspersky Security Center 13.2 Web Console.

To enable forwarding of push notifications through the Kaspersky Security Center 13.2 Web Console:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Notifications** → **Push notifications**.

7. In the **Device name** field, enter the name that will be used by the system to send push notifications.

8. In the **Authorization key** field, enter the authorization code for the device that will receive notifications. For information about obtaining an authorization code, please refer to the Firebase Cloud Messaging

documentation.

9. If you need to add or delete an SSL connection certificate for secure forwarding of notifications to the FCM application, do one of the following:
   - If you need to add a certificate, click the **Upload certificate** button and select a certificate file in the file upload window that appears.

     The certificate file will upload to the system and the information it contains will appear in the profile.
   - If you need to remove a certificate, click the **Remove certificate** button.

     The certificate file will be deleted from the system.
10. Click **Save** in the lower part of the page to save the changes.

Kaspersky IoT Secure Gateway 1000 will send push notifications to authorized devices.

Configuring delivery of MQTT notifications through the Kaspersky Security Center 13.2 Web Console

Kaspersky IoT Secure Gateway 1000 can send notifications about security events and audit events over the MQTT protocol. You can configure delivery of MQTT notifications through the Kaspersky Security Center 13.2 Web Console.

To enable forwarding of MQTT notifications through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Notifications** → **MQTT notifications**.
7. Set the toggle button to **MQTT notifications enabled**.
8. In the **Server address** field, enter the IP address of the utilized MQTT server.
9. In the **Port** field, enter the port number used for the connection with the MQTT server.

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

   You can use port 8883 to connect Kaspersky IoT Secure Gateway 1000 to an MQTT server residing in an external network.
10. In the **MQTT topic name** field, specify the name of the MQTT topic for sending notifications.
11. If you need to send notifications about audit events from a specific user, set the **Use authentication** toggle button to the enabled position and fill in the **User name** and **Password** fields. You can contact the administrator

of the utilized MQTT server to find out the account credentials of the user that will serve as the source of the sent notifications.

Sending notifications from a specific user is disabled by default.

12. If you need to use a secure SSL connection, set the **Use secure SSL connection** toggle button to the enabled position and do the following:

    a. Upload a certificate issued by a Certificate Authority. To do so, click the **Upload certificate** button and select a certificate file on the local device.

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

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

    b. Upload the client certificate. To do so, click the **Upload client certificate** button and select a certificate file on the local device.

    Information about the uploaded client certificate will be displayed on the page.

    c. Upload a key for the client certificate. To do so, click the **Upload key** button and select a key file on the local device.

    Use of a secure SSL connection is disabled by default.

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

Kaspersky IoT Secure Gateway 1000 will send notifications about security events and audit events over the MQTT protocol.

Viewing Kaspersky IoT Secure Gateway 1000 date and time through the Kaspersky Security Center 13.2 Web Console

You can view the date and time of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

To view the date and time of Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Settings** → **Time**.

The opened page displays the date and time of Kaspersky IoT Secure Gateway 1000 received from the device during the last synchronization.

Managing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 13.2 Web Console

This section contains instructions on monitoring events registered in Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

Viewing Kaspersky IoT Secure Gateway 1000 events through the Kaspersky Security Center 13.2 Web Console

You can view events registered by Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

To view events registered by Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway 1000.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Click the **Events** tab.

   This opens a window displaying a table of events registered on the device. The following information is displayed for each table entry:

   - **Time** – date and time when the event was registered.
   - **Event** – type of event.
   - **Severity level** – severity of the event (*Critical*, *Functional failure*, *Warning* or *Informational message*).

Configuring registration of Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 13.2 Web Console

You can enable registration of Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 13.2 Web Console and configure notifications for event registration. For detailed information on configuring notifications for event registration in the Web Console, please refer to the *Configuring notification delivery* section in the Kaspersky Security Center 13.2 Online Help Guide. To configure event registration, first, create a policy for the device from which you plan to receive events. For detailed information on creating a policy, refer to the *Creating a policy* section in the Kaspersky Security Center 13.2 Online Help.

Kaspersky IoT Secure Gateway 1000 version 2.1 does not support management of device groups using Kaspersky Security Center policies. However, you can manage each device separately.

Each event in Kaspersky Security Center has a specific severity level. Depending on the conditions of its occurrence, an event can be assigned one of the following severity levels:

- A *critical event* is an event that indicates the occurrence of a critical problem that may lead to data loss, an operational malfunction, or a critical error.
- A *functional failure* is an event that indicates the occurrence of a serious problem, error or malfunction that occurred during operation of the application or while performing a procedure.
- A *warning* is an event that requires attention because it emphasizes important situations in the operation of Kaspersky IoT Secure Gateway 1000 and may indicate a possible issue in the future. Most events are designated as warnings if the application can be restored without loss of data or functional capabilities after such events occur.
- An *informational message* is an event that informs about successful completion of an operation, proper functioning of the application, or completion of a procedure.

If registration of Kaspersky IoT Secure Gateway 1000 events is disabled in the Web Console, events are not received and are not displayed in the Web Console. After event registration is enabled in the Web Console, only new events will be received. All events that were registered in Kaspersky IoT Secure Gateway 1000 prior to enabling event registration in the Web Console will not be forwarded to the Web Console. Instead, you can view them only in the Kaspersky IoT Secure Gateway 1000 web interface.

To enable registration of Kaspersky IoT Secure Gateway 1000 events in the Kaspersky Security Center 13.2 Web Console:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Click on Kaspersky IoT Secure Gateway 1000.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Click the **Configure events** tab.
6. Select the severity level for which you need to enable event registration:
   - **Critical**.
   - **Functional failure**.

- **Warning**.

- **Informational message**.

   A table of events for the selected severity level will be displayed.

7. Click the **Add event** button.

8. Select the check boxes next to the types of events for which you want to enable event registration in the Web Console, and click **OK**.

9. To save the changes, click the **Save** button.

The selected types of Kaspersky IoT Secure Gateway 1000 events for the selected severity level will be registered and saved on the Kaspersky Security Center Administration Server. The default storage time for events is 30 days.

Configuring 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. You can use the masquerading function if you need to spoof the parameters in the headers of IP packets for devices on the internal network. This allows devices residing in the internal network and not having public IP addresses to send and receive IP packets from an external network.

To enable the masquerading function through the Kaspersky Security Center 13.2 Web Console:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Settings** → **NAT**.

7. Enable or disable the masquerading feature by setting the toggle button to **Masquerading enabled** or **Masquerading disabled** as necessary.

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

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

Updating and restarting Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console

You can update or restart Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

To update or restart Kaspersky IoT Secure Gateway 1000:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Kaspersky Security Center**.
7. If you need to update Kaspersky IoT Secure Gateway 1000, select the **Update** tab and do the following:
   a. In the **Update address** field in the opened window, specify the address of the update package for Kaspersky IoT Secure Gateway 1000 in the following format: http://<server IP address>:<port>/path_to_update_package (for example, http://10.10.100.80/update.pkg).

      > First, on the device hosting the HTTP server, you need to create a firewall rule that allows TCP connections from external network devices via the specified port (for example, port 80).
   b. Select the **Commands** tab.

   c. In the opened window, select **Update** from the **Commands** drop-down list.
   d. Click the **Save** button in the lower part of the page.

      Kaspersky IoT Secure Gateway 1000 updates will be loaded.
8. If you need to restart Kaspersky IoT Secure Gateway 1000, select the **Commands** tab and do the following:
   a. In the opened window, select **Restart** from the **Commands** drop-down list.

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

      Kaspersky IoT Secure Gateway 1000 will be restarted.

Managing the Intrusion Prevention system

Kaspersky IoT Secure Gateway 1000 allows you to detect and prevent suspicious network activity in network traffic on internal and external interfaces using an Intrusion Prevention System (IPS component). Intrusion Prevention rules are applied when analyzing traffic.

An *Intrusion Detection rule* describes a traffic anomaly that could be a sign of an intrusion into the protected infrastructure of an enterprise. Rules contain the conditions that the Intrusion Prevention system uses to analyze traffic and detect signs of the most frequently encountered attacks or suspicious network activity. Intrusion Prevention rules are provided by Kaspersky and are stored in Kaspersky IoT Secure Gateway 1000. They are available immediately after Kaspersky IoT Secure Gateway 1000 is installed.

Kaspersky IoT Secure Gateway 1000 generates a list of denied IP addresses based on traffic analysis using intrusion prevention rules. The list of denied IP addresses contains the internal network's and external network's IP addresses whose network traffic is blocked by Kaspersky IoT Secure Gateway 1000. Kaspersky IoT Secure Gateway 1000 removes a blocked IP address from the list of denied IP addresses one hour after suspicious activity from this IP address ends.

If the Intrusion Prevention System and the list of denied IP addresses are enabled and a rule is triggered, Kaspersky IoT Secure Gateway 1000 automatically blocks traffic from the IP address showing suspicious network activity, registers a security event and writes it to the network security log.

If the Intrusion Prevention System is enabled but the list of denied IP addresses is disabled and a rule is triggered, Kaspersky IoT Secure Gateway 1000 does not block traffic from the IP address showing suspicious network activity but registers a security event and writes it to the network security log.

If the Intrusion Prevention System is disabled, Kaspersky IoT Secure Gateway 1000 does not analyze suspicious network activity.

The list of allowed IP addresses contains the internal network's and external network's IP addresses whose network traffic is not blocked by Kaspersky IoT Secure Gateway 1000. You can add IP addresses of the devices whose traffic should be allowed to the authorized list. If necessary, you can also remove IP addresses of devices from the authorized list.

Enabling and disabling the Intrusion Prevention System

You can enable or disable the Intrusion Prevention System of Kaspersky IoT Secure Gateway 1000. The Intrusion Prevention System is enabled by default.

To enable or disable the Intrusion Prevention System:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **IPS** and set the toggle button to **Intrusion Prevention System is on** or **Intrusion Prevention System is off** as necessary. The Intrusion Prevention System is enabled by default.
7. Click **Save** in the lower part of the window.

Adding an IP address to the list of allowed IP addresses

You can add IP addresses of devices whose network traffic should be allowed to the list of allowed IP addresses.

To add an IP address to the list of allowed IP addresses:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **IPS**.
7. Click the **Show list** button next to the **IP address allowlist** header.

   The **IP address allowlist** window will be displayed.
8. Click the **Add** button.
9. In the **IP address (source)** field that opens on the right, specify the IP address from which you want to allow traffic.
10. Click **OK**, then click **Save** in the lower part of the page.

The device IP address will be added to the list of allowed IP addresses.

Deleting an IP address from the IP address allowlist

You can delete IP addresses of devices from the IP address allowlist.

To delete an IP address from the IP address allowlist:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **IPS**.

7. Click the **Show list** button next to the **IP address allowlist** header.

   The **IP address allowlist** window will be displayed.

8. Select the device IP address that you need to remove from the IP address allowlist and click the **Delete** button in the upper part of the table.

9. Click **OK**, then click **Save** in the lower part of the page.

The selected IP address will be removed from the IP address allowlist.

Enabling and disabling the IP address denylist

In the Kaspersky Security Center 13.2 Web Console, you can enable or disable the list of denied IP addresses if you need to block or allow network traffic coming from these IP addresses.

> If the list of denied IP addresses is disabled, Kaspersky IoT Secure Gateway 1000 identifies IP addresses that show signs of suspicious network activity but does not block them.

To enable the IP address denylist:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Network** → **IPS**.

7. Click the **Show list** button next to the **IP address denylist** header.

   The **IP address denylist** window will be displayed.

8. Set the toggle button to **Apply IP address denylist** or to **Do not apply IP address denylist** as required.

9. Click **OK**, then click **Save** in the lower part of the page.

Managing the firewall

You can use the firewall that is built in to Kaspersky IoT Secure Gateway 1000 to control and filter traffic transversing the device. Network traffic is processed according to *firewall rules* that are defined through the Kaspersky Security Center 13.2 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 1000. You cannot edit these rules, and they are not displayed in the Kaspersky IoT Secure Gateway 1000 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 13.2 Web Console, from top to bottom. You can create up to 1,000 custom firewall rules.

Kaspersky IoT Secure Gateway 1000 supports rules for the TCP and UDP protocols (only IPv4).

Stateful packet inspection is enabled for these protocols. .

Preset rules allow the following Kaspersky IoT Secure Gateway 1000 connections:

- Outgoing connections with the Kaspersky Security Center 13.2 Web Console over the TCP protocol
- Outgoing connections with the update server over the TCP, UDP, and TCP/TLS protocols
- Incoming connections with the local web server over the HTTPS protocol
- Outgoing connections with the Syslog server over the TCP and UDP protocols
- Outgoing and incoming connections with MQTT data sources over the TCP protocol
- Outgoing and incoming connections with external and internal DNS servers over the UDP protocol

Procedure for processing network traffic

Kaspersky IoT Secure Gateway 1000 handles network traffic according to firewall rules and authorized and unauthorized lists, which are defined by the Intrusion Prevention System.

Kaspersky IoT Secure Gateway 1000 applies rules in the following order when processing network traffic:

1. Preset firewall allow rules.
2. List of allowed IP addresses.
3. List of denied IP addresses.
4. Custom firewall rules.
5. Preset firewall block rules.

Creating firewall rules

You can create firewall rules through the Kaspersky Security Center 13.2 Web Console.

> Custom firewall rules are checked in the order defined in the Kaspersky Security Center 13.2 Web Console, from top to bottom until the first match.

To create a new firewall rule:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Firewall**.

   This opens a table containing all the custom firewall rules.
7. Click the **Add** button in the upper part of the firewall rules table.

   The pane for adding a firewall rule will open on the right.
8. In the **Rule status** drop-down list, select the status of the rule: **Enabled** or **Disabled**.
9. In the **Action** drop-down list, select the action to apply to traffic traversing the firewall: **Allow** or **Block**.
10. In the **Zone** drop-down list, select the zone to which the rule should be applied: **LAN** or **WAN**.
11. In the **IP address (source)** field, specify the IP address of the traffic source.
12. In the **Port (source)** field, specify the port of the traffic source if this parameter is applicable to the protocol.
13. In the **IP address (target)** field, specify the IP address of the traffic destination.
14. In the **Port (target)** field, specify the port of the traffic destination if this setting is applicable to the protocol.
15. In the **Protocol** drop-down list, select the utilized protocol. The following protocols are available:
    - **TCP (IPv4)**.
    - **UDP (IPv4)**.
    - **Any**.
16. Click **OK** in the pane for adding a firewall rule.

    The pane will close, and the new rule will be displayed in the firewall rules table.
17. If you need to change the order (priority) of a rule in the rules table, select the check box next to the rule and use the **Up** or **Down** button to raise or lower the rule priority.

18. Click the **Save** button.

Editing firewall rules

You can edit firewall rules through the Kaspersky Security Center 13.2 Web Console.

To edit a firewall rule:

1. In the main window of the Web Console, select **Devices** → **Managed devices**.
2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.
3. In the device properties window that opens, select the **Applications** tab.
4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.
5. Select the **Application settings** tab.
6. Select **Network** → **Firewall**.

   This opens a table containing all the custom firewall rules.
7. Select the check box next to the rule that you want to edit.
8. Click the **Edit** button in the upper part of the firewall rules table.

   The pane for editing a firewall rule opens on the right.
9. If you need to change the status of the rule, select a rule status from the **Status** drop-down list: **Enabled** or **Disabled**.
10. If you need to change how traffic is handled by the firewall, in the **Action** drop-down list, select one of the available actions to apply to traffic traversing the firewall: **Allow** or **Block**.
11. If you need to change the direction of traffic, in the **Zone** drop-down list, select the zone to which the rule should be applied: **LAN** or **WAN**.
12. If necessary, change the IP address of the traffic source in the **IP address (source)** field.
13. If necessary, change the port of the traffic source in the **Port (source)** field if this parameter is applicable to the protocol.
14. If necessary, change the IP address of the recipient in the **IP address (target)** field.
15. If necessary, change the port of the recipient in the **Port (target)** field.
16. If necessary, select a protocol from the **Protocol** drop-down list. The following options are available:
    - **TCP (IPv4)**.
    - **UDP (IPv4)**.
    - **Any**.

17. Click **OK** in the pane for editing a firewall rule.

    The pane will close, and the changes to the rule will be displayed in the firewall rules table.

18. If you need to change the order (priority) of a rule in the rules table, select the check box next to the rule and use the **Up** or **Down** button to raise or lower the rule priority.

    > Custom firewall rules will be checked according to their order in the rules table, from top to bottom until the first match.

19. Click the **Save** button.

Deleting firewall rules

You can delete firewall rules through the Kaspersky Security Center 13.2 Web Console.

To delete a firewall rule:

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

2. Click the name of the device where Kaspersky IoT Secure Gateway 1000 is running. If the device name is not on the list, add it to the **Managed devices** group.

3. In the device properties window that opens, select the **Applications** tab.

4. Press **Kaspersky IoT Secure Gateway**.

   This opens a window containing information about Kaspersky IoT Secure Gateway 1000.

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

6. Select **Network** → **Firewall**.

   This opens a table containing all the custom firewall rules.

7. Select the check box next to the rule that you want to delete.

8. Click the **Delete** button in the upper part of the firewall rules table.

   The rule will be deleted from the firewall rules table.

9. Click the **Save** button.

Contacting Technical Support

If you have any questions about the Advantech UTX-3117-S6A1N hardware system, you are advised to contact the company Merlion, which is the official distributor in Russia, by sending an email to support@merlion.ru ↗. If your issue pertains to only Kaspersky IoT Secure Gateway 1000 and you have not found a solution to the issue in the Kaspersky IoT Secure Gateway 1000 Help Guide, you are advised to contact Aprotech Technical Support by emailing support@aprotech.ru ↗.

To receive additional information about the state of network interfaces and the routing table, you can go to the troubleshooting page at the following address: <Kaspersky IoT Secure Gateway 1000 web interface address>/troubleshooting.html. Information is displayed on the <Kaspersky IoT Secure Gateway 1000 web interface address>/troubleshooting.html page only if you have already logged in to the Kaspersky IoT Secure Gateway 1000 web interface.

Appendices

This section provides additional information to supplement the primary text of the document.

Preparing to install Kaspersky IoT Secure Gateway 1000

Before installing Kaspersky IoT Secure Gateway 1000, you must prepare the Advantech UTX-3117FS-S6A1N device for installation of Kaspersky IoT Secure Gateway 1000.

> Preparations for Kaspersky IoT Secure Gateway 1000 installation are performed by Kaspersky experts. The instructions described in this section are provided for information purposes.

To prepare the Advantech UTX-3117FS-S6A1N device for Kaspersky IoT Secure Gateway 1000 installation:

1. Turn on the Advantech UTX-3117FS-S6A1N device.
2. Connect a monitor and keyboard to the appropriate ports on the front panel of the Advantech UTX-3117FS-S6A1N.
3. 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 device will start running.
4. While the device is loading, press the **DELETE** key on the keyboard.

   The main BIOS menu of the Advantech UTX-3117FS-S6A1N device will open.
5. 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 by pressing **F4**.

   The Advantech UTX-3117FS-S6A1N will begin to restart.
6. During the restart, press the **DELETE** key on the keyboard.

   The main BIOS menu of the Advantech UTX-3117FS-S6A1N device will open.
7. Check the date and time settings.

   a. Select the **Main** tab.

   b. Select **System Date**. If necessary, indicate the correct date.

   c. Select **System Time**. If necessary, indicate the correct time.
8. Modify the secure boot settings of the system:

   a. Select the **Security** tab.

b. Select **Secure Boot**.

c. Depending on the BIOS version on the Advantech UTX-3117FS-S6A1N device, do one of the following:

- Select **Disabled** for the **Attempt Secure Boot** setting.
- Select **Disabled** for the **Secure Boot** setting.

9. Configure the southbridge:

a. Select the **Chipset** tab.

b. Select **South Bridge**.

c. Select **Intel Linux** for the **OS Selection** parameter.

10. On the **Chipset** tab, configure the device to turn on automatically after a sudden power loss:

a. Select **South Cluster Configuration**.

b. Select **Power On** for the **Restore AC Power Loss** setting.

11. Configure the advanced settings:

a. Select the **Advanced** tab.

b. In the opened menu, select **CSM Configuration**.

c. Select **Enabled** for the **CSM Support** setting.

d. For the **Network** and **Other PCI devices Support** settings, select **Do not launch**.

e. Return to the **Advanced** tab by pressing **ESC**.

f. In the opened menu, select **CPU Configuration**. Select **Enabled** for the **VT-d** setting.

g. Return to the **Advanced** tab by pressing **ESC**.

h. In the opened menu, select **Network Stack Configuration**. Select **Enabled** for the **Network Stack** parameter.

i. Return to the **Advanced** tab by pressing **ESC**.

j. In the opened menu, select **Serial Port Console Redirection**.

k. Select **Enabled** for the **Console Redirection** setting.

l. Select **Console Redirection Settings**.

m. Select **VT100+** for the **Terminal Type** setting.

n. Return to the **Advanced** tab by pressing **ESC**.

12. Configure the boot settings:

a. Select the **Boot** tab.

    b. Select **UEFI OS** for the **Boot Option #1** parameter.

13. Exit BIOS while saving the changes:

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

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

The Advantech UTX-3117FS-S6A1N will restart with the configured settings. The device will continue to start with the configured settings on subsequent startups. Before installing Kaspersky IoT Secure Gateway 1000, the device must be shut down.

Installing Kaspersky IoT Secure Gateway 1000

To begin working with Kaspersky IoT Secure Gateway 1000, it must be installed on an Advantech UTX-3117FS-S6A1N device.

> Installation of Kaspersky IoT Secure Gateway 1000 is performed by Kaspersky experts. The instructions described in this section are provided for information purposes.

To install Kaspersky IoT Secure Gateway 1000:

1. Download the SystemRescueCd distribution package image from the official SystemRescue website.

2. On the local computer, create a bootable USB drive containing the SystemRescueCd distribution package, for example, by using the dd utility:

   ```
   $ dd if=systemrescuecd-6.0.3.iso of=/dev/%USB device name%
   ```

   The dd utility is available only in some UNIX™-based operating systems.

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.

5. Press the `DELETE` key on the keyboard.

   The main BIOS menu of the Advantech UTX-3117FS-S6A1N device will open.

6. Configure the settings for loading Kaspersky IoT Secure Gateway 1000 from a bootable USB drive:

   a. Select the **Boot** tab.

   b. In the **Boot Option Priorities** section, use the **+** or **-** key to move the **UEFI: <name_of_bootable_USB>** value to the first position.

   c. Exit the **Boot** tab by pressing **ESC**.

7. Exit BIOS while saving the changes:

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

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

After Kaspersky IoT Secure Gateway 1000 is installed and the bootable USB drive is extracted, the settings defined at this step of the instructions will be reset. The next time Kaspersky IoT Secure Gateway 1000 is loaded, it will apply the load settings that were configured during preparations for Kaspersky IoT Secure Gateway 1000 installation.

8. Go to the directory /tmp by entering the following command in the command line:

   ```
   $ cd /tmp
   ```

9. Download the Kaspersky IoT Secure Gateway 1000 installation image from the internal network, for example, by using the wget utility:

   ```
   $ wget %path to the installation image of Kaspersky IoT Secure Gateway 1000%
   ```

   The Kaspersky IoT Secure Gateway 1000 installation image received in the distribution kit must be put on an HTTP server deployed in the local network in advance.

   The HTTP server and the Advantech UTX-3117FS-S6A1N device must reside in the same network.

10. 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
    ```

11. Start the installation:

    ```
    $ ./install.sh
    ```

12. When installation completes, use the SystemRescueCd tools to shut down the Advantech UTX-3117FS-S6A1N by running the following command:

    ```
    $ shutdown -h now
    ```

13. Eject the bootable USB drive containing the SystemRescueCd distribution package.

14. Turn on the Advantech UTX-3117FS-S6A1N by clicking the on/off button in the right part of the front panel.

Kaspersky IoT Secure Gateway 1000 will start automatically.

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

Error connecting to the Kaspersky IoT Secure Gateway 1000 web interface

Problem

When connecting to the Kaspersky IoT Secure Gateway 1000 web interface using the supported Google Chrome web browser, the login page for the Kaspersky IoT Secure Gateway 1000 web interface does not load.

Solution

To successfully connect to the Kaspersky IoT Secure Gateway 1000 web interface using the Google Chrome web browser, your operating system must use the standard system port range for TCP connections.

Some applications that may be installed on your personal computer running a Windows® operating system may have changed the default system port range that is used to connect over the TCP protocol.

To successfully connect to the Kaspersky IoT Secure Gateway 1000 web interface using the Google Chrome web browser:

1. Open a console on the computer where you are trying to connect to the Kaspersky IoT Secure Gateway 1000 web interface.
2. In the console run the following command, which will display the range ports that are used by the system for TCP protocol connection:

   ```
   netsh int ipv4 show dynamicport tcp
   ```

   The console will display the port range used for the TCP protocol.
3. If the displayed port range starts with port 1024, then run the following command as an administrator to restore the system port range for the TCP protocol to its default values:

   ```
   netsh int ipv4 set dynamicport tcp start=49152 num=16384
   ```
4. Try again to connect to the Kaspersky IoT Secure Gateway 1000 web interface using the Google Chrome browser.

   The Kaspersky IoT Secure Gateway 1000 login page opens.

Glossary

Administration Server

A Kaspersky Security Center entity that centrally stores information about all Kaspersky applications that are installed within an enterprise network. It can also be used to manage these applications.

Administrator certificate

A certificate used for user authentication in the Kaspersky IoT Secure Gateway 1000 web interface.

Application administration plug-in

A specialized entity that provides an interface for application management through the Administration Console. Each application has its own administration plug-in. It is included in all Kaspersky applications that can be managed using Kaspersky IoT Secure Gateway 1000.

Event

A record containing information about 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 1000 entity

A part of Kaspersky IoT Secure Gateway 1000 that is designed to provide system functionality (such as authentication).

Kaspersky Security Center 13.2 Web Console

A web application designed to manage the state of the security system of enterprise networks that are protected by Kaspersky applications.

Kaspersky Security Center administrator

The person who manages application operations through the remote centralized administration system known as Kaspersky Security Center.

KasperskyOS

A microkernel operating system used for building secure solutions.

KSC server certificate

A certificate that is used for secure interaction between Kaspersky IoT Secure Gateway 1000 and Kaspersky Security Center when managing Kaspersky IoT Secure Gateway 1000 through the Kaspersky Security Center 13.2 Web Console.

Managed devices

Enterprise network devices that are included into an administration group.

Message Queuing Telemetry Transport (MQTT)

A network protocol that works on top of the TCP/IP protocol stack to exchange messages between devices on the Internet of Things.

MQTT broker

A server that receives, filters, and forwards messages over the MQTT protocol.

MQTT-topic

A hierarchical path to the data source used for sending messages over the MQTT protocol.

SSL

A protocol for data encryption in local networks and on the Internet. SSL is used in web applications to create secure connections between a client and a server.

TLS

Secure protocol that uses encryption to transfer data in local networks and on the Internet. TLS is used in web applications to create secure connections between a client and a server.

UEFI protection device

A device with Kaspersky Anti-Virus for UEFI integrated at the BIOS level. Integrated protection ensures device security from the moment the system starts. In contrast, devices without integrated software are protected only after the security application starts.

Third party code information

Third party code information is contained in the file named legal_notices.txt, which is located on the local web server. You can open the file from the **About** section.

Trademark notices