



# Kaspersky IoT Secure Gateway 1000 Feature list

**Kaspersky IoT Secure Gateway 1000** helps to build secure and functional internet of things systems. This KasperskyOS-based gateway is Cyber Immune, which means it will perform its critical functions even in an aggressive environment.

KISG 1000 serves as a reliable connection point between IoT devices and cloud platforms, protects the infrastructure from cyberattacks and makes it transparent. The gateway securely collects data and transfers it to the cloud via the MQTT over TLS protocol.

The **Kaspersky Security Center** console enables convenient centralized monitoring and administration of all KISG 1000 events. Together, the two products form the comprehensive **Kaspersky IoT Infrastructure Security** solution.

Learn more on [os.kaspersky.com](https://os.kaspersky.com)

| Hardware platform           | Advantech UTX-3117                           |
|-----------------------------|--|
| Processor                   | Intel Pentium N4200, 1.1GHz, 2MB L2 Cache    |
| RAM                         | 4GB, DDR3L, 1600MHz                          |
| Drives                      | SATA II SSD (32 GB), 2xMiniPCIe, 1xM.2 B-key |
| Interfaces                  | 2xGbE LAN                                    |
| Dimensions                  | 128x152x37mm                                 |
| Operating temperature range | -20 to 60°C                                  |
| Extras                      | SIM card                                     |

| Connection      |  |
|-----------------|--|
| Ethernet        | Two gigabit interfaces for connecting to different network segments via a twisted pair (LAN and WAN)                             |
| Cellular modem  | Mobile data network as the primary or backup data channel  |
| Routing and NAT | Automatic routing between KISG 1000 interfaces NAT managing (masquerading)   |
| DHCP server     | Automatic propagation of network configuration to IoT and other devices on the local network                                     |
| MQTT broker     | Mosquitto-based MQTT broker allowing centralized collection of data from IoT devices (sensors and actuators, smart relays, etc.) |

|  |  |
|--|--|
| <b>OpenSSL/TLS</b>                     | Support of common mechanisms for cryptographic protection of data transmitted via the MQTT (Syslog) protocol |
| <b>MQTT over TLS</b>                   | Secure connection and protected transmission of data between the gateway and the cloud platform              |
| <b>Integration with cloud services</b> | MS Azure, Amazon AWS, IBM Bluemix, etc.<br>Works with any cloud systems using the MQTT protocol              |

## Flexible security and gateway management

|                                      |  |
|--------------------------------------|--|
| <b>Web interface</b>                 | User-friendly configuration and monitoring of the IoT network, visibility and transparency thanks to WebGUI. Informative dashboard allows you to get all the information you need quickly  |
| <b>Centralized management system</b> | The Kaspersky Security Center platform allows managing events received from all KISG 1000 units deployed within the organization's infrastructure. It also allows tracking the status of gateways and managing their configuration |

## IoT gateway protection against cyberattacks

|                         |   |
|-------------------------|---|
| <b>Secure by design</b> | The Cyber Immune KasperskyOS operating system rules out device compromise, thus making a data leak or penetration of the enterprise infrastructure impossible   |
| <b>Secure boot</b>      | Verification of the integrity and authenticity of gateway firmware using cryptographic methods before loading the image. Firmware that is damaged or altered without authorization will not be loaded |
| <b>Secure update</b>    | Working in conjunction with Secure boot, this technology allows updating the firmware with properly signed and encrypted images only  |

## IoT infrastructure protection

|  |  |
|--|--|
| <b>IDS/IPS and firewall</b>  | The firewall uses the principle of Default Deny. The administrator can rest assured that only allowed network interactions will pass through the gateway.<br>The IDS/IPS (Intrusion Detection and Prevention) module blocks malicious activity detected using a signature set prepared by Kaspersky specialists, and notifies the administrator        |
| <b>Detection and classification of IoT devices</b>   | Detects devices on the local network by their network activity.<br>The user interface can display all the network devices already interacting with KISG 1000, while new ones will be detected within 60 seconds  |
| <b>Reports and notifications (MQTT, Syslog, push notifications, Kaspersky Security Center)</b> | The administrator can receive KISG 1000 security events in a single enterprise security management system (Kaspersky Security Center), and transmit events to external systems (SIEM, cloud platforms, etc.) using the Syslog and MQTT protocols. KISG 1000 supports integration with Google Firebase for sending push notifications to mobile devices |



**KasperskyOS**



**Kaspersky  
IoT Secure  
Gateway 1000**

Learn more on [os.kaspersky.com](https://os.kaspersky.com)

[www.kaspersky.com](https://www.kaspersky.com)

© 2021 AO Kaspersky Lab.  
Registered trademarks and service marks are the property of their respective owners.