kaspersky

Kaspersky Industrial CyberSecurity for Networks

Contents

About Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks is an application designed to protect the infrastructure of industrial enterprises from information security threats, and to ensure uninterrupted process flows. Kaspersky Industrial CyberSecurity for Networks analyzes industrial network traffic to identify deviations in the values of process parameters, detect signs of network attacks, and monitor the operation and current device states on the network. The application is part of the solution known as Kaspersky Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Networks performs the following functions:

- Protects company assets by monitoring its industrial network devices. Detects device activity and device information based on data received from network packet analysis and/or from Kaspersky applications that perform functions to protect workstations and servers.
- Controls devices and interaction between them with respect to their MAC addresses or IP addresses affiliation with address spaces.
- Scans communications between industrial network devices to check their compliance with defined Interaction Control rules. Interaction Control rules can be generated automatically by running the application in learning mode.
- Displays interactions between industrial network devices as a network interaction map. Displayed objects are visually distinguished based on various attributes (for example, objects with issues).
- Displays a diagram of the physical connections between devices in an industrial network as a topology map. Displayed objects are visually distinguished by various attributes (for example, by the status).
- Detects risks based on traffic analysis and received information on devices.
- Allows running active polling of devices using connectors to obtain the most accurate and complete information about devices and their configuration.
- Allows you to conduct a device security audit to assess device compliance with the security standards and perform other checks.
- Extracts the parameter values of the technological process controlled by the Industrial Control System (hereinafter referred to as the "ICS") from network packets and checks the acceptability of those values based on the defined Process Control rules. Process Control rules can be generated automatically by running the application in learning mode.
- Monitors traffic to detect system commands that are transmitted or received by devices involved in process automation. Provides notifications regarding detected unauthorized system commands or situations that could be signs of industrial network security violations.
- Monitors project read and write operations for programmable logic controllers, saves the obtained information about projects, and compares this information to previously obtained information.
- Analyzes industrial network traffic for signs of attacks without affecting the industrial network or drawing the attention of a potential attacker. Uses defined Intrusion Detection rules and embedded algorithms to scan for anomalies in network packets and detect signs of attacks.
- Registers network sessions created by the devices for connecting with other devices.
- Registers events and relays information about them to recipient systems and to Kaspersky Security Center.
- Analyzes registered events and, upon detecting certain sequences of events, registers incidents based on embedded correlation rules. Incidents group events that have certain common traits or that are associated

with the same process.

- Saves traffic associated with registered events in the database. Traffic can be saved automatically (if autosave is enabled for the traffic of events) or by requesting to download traffic.
- Receives and processes data from the applications that are part of the Endpoint Protection Platform (EPP). Registers events and risks when data is received from EPP applications. Displays information about threat development chains in the events that are Endpoint Detection and Response incidents.
- Provides the capability to trigger response actions for the devices with Kaspersky Endpoint Agent installed.
- Provides reports on the device status and system security, as well as the results of a security audit.
- Provides the capability to download traffic from the storages of the traffic dump files. Both the internal node storage (created automatically) and the external node storage, if connected on the node, can be used to download traffic.
- Can be used to work with both the GUI and API.
- Provides data for centralized monitoring of systems with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console.

Distribution kit

The distribution kit of Kaspersky Industrial CyberSecurity for Networks includes the following files:

- An archive containing all files of the application distribution kit: kics4net-release_<application version>.tar.gz
  The archive contains the following files:
  - ZIP archives with descriptions of connector types built into the application (located in "connector-types" packaged directory)
  - Scripts and packages for installing, validating and removing application components (located in "linux-centos" packaged directory)
  - Packages for installing Kaspersky Industrial CyberSecurity for Networks administration plug-in for Kaspersky Security Center and Kaspersky Industrial CyberSecurity for Networks administration web plug-in for Kaspersky Security Center Web Console (located in "sc_plugin" packaged directory)
  - Archives with documentation describing requests and specifications for Kaspersky Industrial CyberSecurity for Networks API (located in "sdk" packaged directory)
  - Files containing the text of the End User License Agreement in English and in Russian
  - Files containing the text of the Privacy Policy in English and in Russian
  - Files containing information about the version (Release Notes) in English and in Russian
- Copies of files contained in the kics4net-release_<application version>.tar.gz archive:
  - Packages for installing Kaspersky Industrial CyberSecurity for Networks administration plug-in for Kaspersky Security Center and Kaspersky Industrial CyberSecurity for Networks administration web plug-in for Kaspersky Security Center Web Console

- Files containing the text of the End User License Agreement in English and in Russian
- Files containing the text of the Privacy Policy in English and in Russian
- Files containing information about the version (Release Notes) in English and in Russian

Hardware and software requirements

Hardware requirements

Kaspersky Industrial CyberSecurity for Networks has the following minimum hardware requirements for computers on which application components will be installed:

- Computer that will perform Server functions:
  - CPU: Intel® Core™ i7 or equivalent (highest single-core frequency configurations are recommended)
  - RAM: 32 GB
  - Free space on the hard drive: 500 GB (SSD is recommended)
- Computer that will perform sensor functions:
  - CPU: Intel Core i5 / i7 or equivalent (maximum core configurations are recommended)
  - RAM: 8 GB, and an additional 2 GB for each monitoring point on this computer
  - Free space on the hard drive: 250 GB (SSD is recommended)

The maximum speed of inbound traffic at all monitoring points of the Server must be no more than 500 Mbps. For stable performance and to prevent data loss from incoming traffic in a distributed network architecture, it is recommended to use the deployment scheme that involves the Server and external sensors. Sensors reduce the load on the Application Server thanks to traffic preprocessing and data storage.

The maximum speed of incoming traffic at all of a sensor's monitoring points must be no more than 250 Mbps. When using sensors in a network with a distributed network architecture, it is recommended to configure receiving all industrial network traffic at a sensor's monitoring points and not at the Server.

> If the devices originating the traffic also send duplicate traffic to another network interface of the Server or sensor, the application automatically discards duplicate network packets. However, the application's actions when processing network packets in this way increase the load on the computer's hardware resources and in some cases may slow down traffic processing.

When using sensors, the bandwidth of the dedicated Kaspersky Industrial CyberSecurity network between the Server and each sensor must be at least 1 Mbps, excluding the speed of the traffic coming to the sensor monitoring points. Considering the speed of the traffic coming to the monitoring points, the bandwidth of the channel between the sensor and the Server must be increased by at least 50% of the total incoming traffic to the sensor (for all monitoring points of the sensor).

> Example:
> A sensor has two monitoring points. One monitoring point receives 100 Mbps of traffic, while the other receives 200 Mbps. In this case, the bandwidth of the channel between the sensor and the Server must be at least 151 Mbps (1+(200+100)/2=151).

Software requirements

Kaspersky Industrial CyberSecurity for Networks has the following software requirements for computers on which application components will be installed:

- CentOS Stream 9 operating system.

  > When installing the operating system, it is recommended to allocate the entire hard drive (minus the minimum space required for the boot and swap partitions) to the system (root) partition. To improve the performance of software, you can also mount the /var/ folder to a high-speed hard drive (if you have an additional drive, such as an SSD drive). If you choose to do so, the /var/ folder must be completely mounted to the other drive. Subfolders within the /var/ folder (such as /var/opt/) cannot be mounted to different drives.

- The same version of operating system must be installed on all computers where application components are installed.

- To install application components in the CentOS operating system, the following conditions must be fulfilled:

- Chrony time synchronization package version 3.1 or later is installed

  You can install the Chrony time synchronization package by using the following commands in the operating system console:

  ```
  sudo dnf install chrony
  sudo systemctl enable chronyd
  sudo systemctl start chronyd
  ```

- The SELinux access control enforcement system is disabled

  1. Open the system configuration file. To do so, enter the following command:

     ```
     sudo mcedit /etc/selinux/config
     ```

  2. Set the following parameter value:

     ```
     SELINUX=disabled
     ```

  3. Save and close the configuration file.

  4. Restart the computer.

- The dnf-utils package is installed

  You can install the dnf-utils package by using the following command in the operating system console:

  ```
  sudo dnf install dnf-utils
  ```

- The compat-openssl package is installed

  You can install the compat-openssl package by running the following command in the operating system console:

  ```
  sudo dnf install compat-openssl11
  ```

- The lttng-ust package with the LTTng library version no newer than 2.12 is installed

  In CentOS Stream 9 operating system, you can install the lttng-ust package with the required version of the LTTng library using the following command in the operating system console:

  ```
  sudo dnf install lttng-ust.x86_64
  ```

- To ensure proper functioning of application components on the computer that will perform Server functions, the following conditions must also be fulfilled in the CentOS operating system:

  - Python interpreter version 3.9 or later is installed, along with packages supporting the operation of connectors and data conversion scripts (if connectors will also operate on other computers, the packages must also be installed on those computers)

    You can install packages for connectors and data conversion scripts by carrying out the following commands in the operating system console:

    ```
    sudo dnf install epel-release

    sudo dnf install python3-psycopg2 python3-cryptography python3-paramiko
    ```

  - Mail server is installed (Mail Transfer Agent, MTA) to send emails through the email connector and to send reports by email (for example, Postfix)

    You can install a Postfix mail server by using the following commands in the operating system console:

    ```
    sudo dnf -y install postfix
    sudo systemctl start postfix
    sudo systemctl enable postfix
    ```

  - Perl interpreter version 5.10 or later is installed (if Kaspersky Security Center Network Agent is being installed).

> For installation of application components, it is recommended to use separate computers on which only software from the operating system is installed. If third-party applications are installed on computers, the performance of components of Kaspersky Industrial CyberSecurity for Networks may be reduced.

You can use the following browsers to connect through the web interface:

- Google Chrome™ version 115 or later.
- Mozilla™ Firefox™ version 116 or later.
- Microsoft® Edge® version 115 or later.

Kaspersky Industrial CyberSecurity for Networks is compatible with Kaspersky Security Center 14.2 and Kaspersky Security Center 15 Linux.

Kaspersky Industrial CyberSecurity for Networks supports operation in the integration mode with the following applications: Kaspersky Industrial CyberSecurity for Nodes 3.1 and 3.2 and Kaspersky Industrial CyberSecurity for Linux Nodes version 1.3. In the integration mode, Kaspersky Industrial CyberSecurity for Networks interacts with Kaspersky Endpoint Agent installed on the devices. When interacting with Kaspersky Endpoint Agent, the following functionalities are available in Kaspersky Industrial CyberSecurity for Networks:

- Receiving basic data about the devices and running processes (telemetry data).
- Receiving extended data about the devices and running processes: data for equipment monitoring, data for determining device categories, and data for building threat chains.
- Performing actions on devices: scanning devices as part of security audit jobs, triggering response actions.

Receiving basic data (telemetry data) is available when using Kaspersky Endpoint Agent 3.14 or later. The capabilities of receiving extended data and performing actions on devices are available when using Kaspersky Endpoint Agent 3.15 or Kaspersky Endpoint Agent 3.16. However, to interact with Kaspersky Endpoint Agent 3.15, you must use version 3.15.0.279 with the patch installed, which activates the functionality of integration with Kaspersky Industrial CyberSecurity for Networks. You can request Kaspersky Endpoint Agent 3.15.0.279 and the patch for this version from your personal technical account manager (TAM).

Overview of Kaspersky Industrial CyberSecurity for Networks functionality

Industrial network traffic analysis functionality

In Kaspersky Industrial CyberSecurity for Networks, industrial network traffic analysis is provided by the following functionality:

- **Asset Management**. This functionality lets you monitor the activity of devices and track changes to device information based on data received in network packets. To automatically receive information about devices, the application analyzes industrial network traffic according to the rules for identifying information about devices and the protocols of communication between devices. The application can also define device settings for Process Control. In conjunction with Process Control functionality, read/write operations for programmable logic controllers are also monitored. For the purpose of Asset Management, the application generates a table containing information that is received automatically from traffic or information that is manually provided.
- **Interaction Control**. This functionality lets you monitor interactions between devices of the industrial network. Detected interactions are checked to see if they match any Interaction Control allow rules. When the application detects an interaction that is described in an enabled rule, it considers this interaction to be allowed and does not register an event.
- **Deep Packet Inspection** (hereinafter also referred to as "Process Control"). This functionality lets you monitor traffic to detect the values of process parameters and the systems commands transmitted or received by devices. Values of industrial process parameters are tracked with the aid of Process Control rules that are used by the application to detect unacceptable values. Lists of monitored system commands are generated when you configure the settings of Process Control devices.
- **Intrusion Detection**. This functionality lets you monitor traffic to detect signs of attacks or unwanted network activity. For detection, the following tools are used: intrusion detection rules, built-in network packet scanning algorithms, and the rules for analyzing network activity statistics. When the conditions defined in the rule or described in the scan algorithm are detected in the traffic, the application registers an event based on the Intrusion Detection technology.

Only an application user with the Administrator role can configure industrial network traffic analysis functionality.

Functionality for performing common operator tasks

Application user accounts with the Operator role can be used to perform common tasks for monitoring the state of the industrial process and devices in Kaspersky Industrial CyberSecurity for Networks. These users can utilize the following functionality:

- **Display information for system monitoring in online mode**. This functionality lets you view the most significant changes to the system that have occurred up to the current moment. When the system is being monitored in online mode, you can monitor hardware resource consumption, various dynamic data, and the main information about devices and events.
- **Displaying data on the network interactions map**. This functionality lets you visually display detected interactions between devices of the industrial network. When viewing the network interactions map, you can quickly identify problematic objects or objects with other attributes and view information about these objects. To conveniently present information, you can arrange devices on the network interactions map automatically or manually. In addition to the functionality of the network interaction map, the application displays a table of network sessions, thus providing more capabilities for investigating incidents and analyzing network connection statistics.
- **Displaying data on the topology map**. This functionality lets you visually display a diagram of the physical connections between devices in the industrial network. When viewing the topology map, you can study the structure of connections between devices via network equipment and view information about devices and their connections. To conveniently present information, you can arrange devices on the topology map automatically or manually.
- **Display information about events and incidents**. This functionality lets you download registered events and incidents from the Server database and display this information as an events table or as interacting objects on a network interactions map. To provide the capability to monitor new events and incidents, by default the application loads events and incidents that occurred most recently. You can also load events and incidents for any period. When viewing the events table, you can change the statuses of events and incidents, copy and export data, load traffic, and perform other actions.
- **Display tag values in online mode**. This functionality lets you view the current values of process parameters detected in traffic at the current point in time. Information about received values is displayed in the tags table generated for Process Control.
- **Display information about detected risks**. This functionality let you detect risks that could affect information system resources. The application detects risks based on traffic analysis and received information on devices. Information about risks can be viewed when managing devices or in the general risks table.
- **Display information for centralized monitoring in the Kaspersky Security Center Web Console**. This functionality lets you view data on the security state of information systems that are running application components (including deployment scenarios involving multiple Kaspersky Industrial CyberSecurity for Networks Servers). When working with the Kaspersky Security Center Web Console, you can view information in web widgets and on component deployment maps, search devices and events in Kaspersky Industrial CyberSecurity for Networks, and quickly navigate from the Kaspersky Security Center Web Console directly to the web interface pages of Servers.

Functionality for managing operation of the application

To manage the application for the purpose of general configuration and control of its use, an application user with the Administrator role can use the following functionality:

- **Manage deployment settings on nodes**. This function allows you to add sensor nodes and monitoring points to the application to receive traffic, manage technologies, and change other deployment settings. You can pause and resume monitoring of industrial network segments, enable technology learning mode, enable and disable technologies, and configure the settings for saving application data on nodes.

- **Manage address spaces**. This functionality lets you control devices and interactions between them with respect to their MAC addresses or IP addresses affiliation with address spaces. You can also use this functionality to check detected IP addresses against the list of subnets of address spaces. You can configure the settings of rules and subnets of address spaces.

- **Performing active polling of devices**. This functionality lets you run active polling of devices using connectors to obtain the most accurate and complete information about devices and their configurations directly from the devices themselves. Performing active polling of devices is only available after adding a license key to Kaspersky Industrial CyberSecurity for Networks. You can specify the information you want to get about devices using active polling, and you can also choose the method for obtaining that information.

- **Performing device security audit**. This functionality lets you assess device compliance with security standards and perform other checks (for example, search for vulnerabilities or detect installed software on devices). Performing device security audit is only available after adding a license key to Kaspersky Industrial CyberSecurity for Networks. You can manually run security audit jobs or configure a schedule to automatically run each job. The application can generate reports with the results of device scans according to security audit rules.

- **Operation with EPP applications**. This functionality lets you select the nodes with installed application components that will receive and process data from Kaspersky applications that perform functions to protect workstations and servers. These applications are included in the Endpoint Protection Platform (EPP) and are installed to endpoint devices within the enterprise IT infrastructure. When data is received from EPP applications, Kaspersky Industrial CyberSecurity for Networks can register events, add devices, and update device information. When working with Kaspersky Endpoint Agent in Kaspersky Industrial CyberSecurity for Networks, the following actions can be performed on devices: scanning devices as part of security audit jobs and triggering response actions.

- **Distribute access to application functions**. This functionality lets you restrict user access to application functions. Access is restricted based on the roles of application user accounts.

- **Monitor the state of the application**. This functionality lets you monitor the current state of Kaspersky Industrial CyberSecurity for Networks, and view application messages and user activity audit entries for any period. Users with the Operator role can also access the log containing application messages.

- **Updating databases and application modules**. This functionality lets you download and install updates, thereby improving the effectiveness of traffic analysis and ensuring maximum protection of the industrial network against threats. Update functionality is available after a license key is added to Kaspersky Industrial CyberSecurity for Networks or to Kaspersky Security Center. You can manually start installation of updates, or enable automatic installation of updates according to a defined schedule.

- **Configure the types of registered events**. This functionality lets you generate and configure a list of event types for event registration in Kaspersky Industrial CyberSecurity for Networks, and for event transmission to recipient systems (for example, to a SIEM system) and to Kaspersky Security Center.

- **Manage logs**. This functionality lets you change the settings for saving data in application logs. You can configure the settings for saving entries in logs and the settings for saving traffic in the database. You can also change the logging levels for process logs. The traffic dump files saved on nodes with the installed application components can be configured to be recorded and stored both in the internal storage and in the external storage. If necessary, you can download traffic from storages to PCAP files.

- **Manage reports**. This functionality allows you to generate reports based on report templates (report templates are used to get information about the status of the information system) and based on the results of device scans during security audits. When configuring the settings for receiving reports, you can specify the report recipients and configure the schedule settings for the automatic generation of reports. You can also manually start generating reports and download the received files. Users with the Operator role have access to the generated reports.

- **Use the application programming interface**. This functionality lets you use the set of functions implemented through the Kaspersky Industrial CyberSecurity for Networks API in external applications. Using the Kaspersky Industrial CyberSecurity for Networks API, you can obtain data on events and tags, send events to Kaspersky Industrial CyberSecurity for Networks, and perform other actions.

Security recommendations for Kaspersky Industrial CyberSecurity for Networks

To ensure secure operation of the application at an enterprise after installation of Kaspersky Industrial CyberSecurity for Networks, it is recommended to reinforce the security of computers on which the Kaspersky Industrial CyberSecurity for Networks Server and sensors are installed. The required level of security ensuring safe operation of the application must be supported by the operating system and its protection tools. To maintain security of the application, it is recommended to regularly install updates for application modules and databases of Kaspersky Industrial CyberSecurity for Networks and security updates for the operating system.

It is recommended to restrict physical access to hardware on which the application is running to prevent the following potential security issues:

- Unauthorized shutdown of hardware (or disconnection from the network)
- Connection of tools that can intercept transmitted data
- Theft of hard drives containing data
- Use of other equipment to destroy or replace data on hard drives

When deploying Kaspersky Industrial CyberSecurity for Networks, you are advised to do the following:

- Restrict remote and local access to computers that have components of Kaspersky Industrial CyberSecurity for Networks installed.

  > After each use of a script for centralized installation of application components (including for centralized removal or to reinforce computer security) you must block access to computers over the SSH protocol for security purposes. You can block access by using the following command in the operating system console: `sudo systemctl disable --now sshd`. To restore access over the SSH protocol (if you need to reuse a script for centralized installation of application components), you can use the command: `sudo systemctl enable --now sshd`.

- Regularly check and update password policies for active user accounts in operating systems on computers that have application components installed. Password policies must comply with the recommendations on ensuring the required level of security of the operating system.
- Ensure that the application interfaces can be accessed only by personnel who are authorized to install and configure the application, and by users (operators) who use the application to perform standard tasks.
- Use hardware or a security service to control physical access to the equipment running the application and to the utilized network equipment.
- Use video surveillance and alarm systems to monitor restricted rooms.

When application events are transmitted to recipient systems (other than Kaspersky Security Center), the application does not guarantee the security of the data transfer. We recommend that you use other means to secure the data transfer.

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

- Protect traffic within the local intranet.
- Protect connections to external networks.
- Use digital certificates published by trusted certificate authorities.
- Use account credentials that meet the requirements for user names and passwords of application user accounts.
- Ensure that passwords are confidential and unique.

  If there is a risk that the password was compromised, the application user must promptly change their password.
- Customized time synchronization on the Kaspersky Industrial CyberSecurity for Networks nodes.
- Terminate the web interface connection session before closing your browser.

  To force termination of a connection session, you need to use the **Log out** option in the user menu.

What's new

Kaspersky Industrial CyberSecurity for Networks 4.1 has the following new capabilities and refinements:

- The security audit functionality is added to assess device compliance with security standards and perform other checks on devices. Device scans can be performed using Kaspersky Endpoint Agent or by remote connection to devices via the protocols that ensure secure management and data transfer. For the safe storage and use of the identification and authentication information, a secret storage is implemented in the application. Detailed information about the results of running security audit jobs is provided in the reports that can be generated automatically or manually.

- The functionality of asset control is expanded in terms of monitoring device equipment. Based on data from EPP applications, as well as during active polls, the application receives and displays more information about the equipment (information about processors, RAM, local disks) and additionally updates information obtained during traffic analysis or entered manually. When the equipment is changed or new information is received during equipment monitoring, the application registers the corresponding events.

- The application capabilities are expanded in terms of determining device categories. Additional algorithms are implemented for more accurate category identification based on data from EPP applications and on the results of traffic analysis.

- The functionality for displaying EDR incidents is added. The events based on EPP technology display information about threat development chains received from Kaspersky Endpoint Agent. When viewing the activity events included in the threat development chain, you can use links with file hashes and URLs to obtain information about the reputation of these objects on the Kaspersky Threat Intelligence Portal. You can export data about the activity events to the indicator of compromise files (IOC files) for further use in the IOC search tasks performed using Kaspersky Endpoint Agent.

- Capabilities to trigger response actions are added. On the devices with Kaspersky Endpoint Agent installed, you can trigger response actions to prevent or minimize the impact of the detected threats from devices (for example, enable network isolation of the device). Response actions can be triggered both when working with events and when working with devices. At the same time, all provided response actions are available when working with events that are EDR incidents (events for which the threat development chains are built).

- Display information about network sessions as a table. In addition to the functionality of the network interaction map, the application displays a table of network sessions, thus providing more capabilities for investigating incidents and analyzing network connection statistics. To fill the table with data, the Network Session Detection method is added to the application; this method can be enabled or disabled.

- The Brute-force Attack and Scan Detection method is added to the Intrusion Detection technology. This method is used to analyze network activity statistics in order to detect signs of credentials brute force attacks, denial of service, scanning, network service spoofing, and other anomalies. The method uses built-in rules. When the rules are triggered, the application registers events based on the Intrusion Detection technology.

- Capabilities for managing technologies are expanded. To gradually commission the application components, you can enable or disable technologies separately on the Server and sensor nodes, as well as on the monitoring points. When configuring the technology usage modes, you can specify the date and time of the automatic switch from the training mode to the monitoring mode.

- The capability to download traffic received at monitoring points is added. The traffic is downloaded from the internal storages with the traffic dump files on the Server and sensors nodes, as well as from the external storages if they are connected at the nodes. For downloading traffic, you can use various options to filter network packets, including defining a period for which to download traffic, and filtering expressions. You can download traffic from storages when viewing information about nodes and monitoring points, as well as when viewing the table of network sessions and when working with a network interactions map.

- The graphical user interface is improved. The useful space is increased for displaying information and parameters of the selected elements in the details areas.

- The list of supported types of external projects for import is extended. New types of projects containing configurations of process control settings for devices can be imported into the application.

- Extended support for application layer protocols and devices for process control – there are now additional capabilities for analyzing traffic of supported protocols and devices, and new supported protocols and devices have been added.

Application architecture

Kaspersky Industrial CyberSecurity for Networks includes the following components:

- The *Server* is the main component that receives data, processes it, and provides it to users of the application. The received information (such as events and device information) is saved on the Server in the database. Only one Server can be used in each Kaspersky Industrial CyberSecurity for Networks deployment scenario.
- A *sensor* is a component that is managed by the Server and receives and analyzes data from computer networks that are connected to the network interfaces of the sensor's computer. A sensor forwards the data analysis results to the Server. Based on the specific requests from the Server, the sensor can forward data in the same format in which the data was received for analysis (for example, traffic related to registered events). Sensors are installed on separate computers. A sensor cannot be installed on a computer that performs Server functions. The application can have up to 50 sensors.

The connections between the Server and sensors are secured by using certificates. Use of certificates also ensures the security of other connections with application components (for example, a connection to a component through a web interface or connections of recipient systems through specialized application modules called *connectors*).

The Kaspersky Industrial CyberSecurity for Networks Server performs the following functions:

- Manages sensors and receives the results of their analysis of data received from computer networks.
- Processes and saves received information about devices and their interactions.
- Receives data from Kaspersky applications that perform functions to protect workstations and servers (EPP applications).
- Interacts with the Kaspersky Endpoint Agent application installed on devices.
- Establishes remote connections to devices to scan those devices as part of security audit jobs.
- Registers and saves events.
- Conducts an additional analysis of accumulated information to detect threats and incidents (for example, according to event correlation rules).
- Monitors application performance.
- Monitors the activities of application users.
- Processes incoming requests submitted through the web interface and connectors, and provides the requested data.

A Kaspersky Industrial CyberSecurity for Networks sensor performs the following functions:

- Analyzes incoming industrial network traffic:
  - Extracts information about device communications and process parameters from traffic.
  - Identifies signs of attacks in traffic.
- Receives data from Kaspersky applications that perform functions to protect workstations and servers (EPP applications).

- Interacts with the Kaspersky Endpoint Agent application installed on devices.
- Establishes remote connections to devices to scan those devices as part of security audit jobs.
- Registers events based on the results of data analysis.
- Relays events, information about traffic, device information, and process parameters to the Kaspersky Industrial CyberSecurity for Networks Server.

Application components receive a copy of industrial network traffic from *monitoring points*. Monitoring points can be used on sensors as well as on the Server. You can add monitoring points to network interfaces detected on nodes that have application components installed. Monitoring points must be added to network interfaces that relay traffic from the industrial network.

You can add no more than 8 monitoring points on a sensor and no more than 4 monitoring points on the Server. You can use no more than 50 monitoring points total in the application.

> All network interfaces with added monitoring points must be connected to the industrial network in such a way that excludes any possibility of impacting the industrial network. For example, you can connect using ports on industrial network switches configured to transmit mirrored traffic (Switched Port Analyzer, SPAN).

It is recommended to use a *dedicated Kaspersky Industrial CyberSecurity network* for connecting the Server to sensors and to other components of Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes, Kaspersky Security Center). Network equipment used for interaction between components in the dedicated network must be installed separately from the industrial network. Normally, the following computers and devices should be connected to the dedicated network:

- Kaspersky Industrial CyberSecurity for Networks Server node.
- Kaspersky Industrial CyberSecurity for Networks sensor nodes.
- Computers for connecting to the Server and sensors through the web interface.
- Computers with Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes and Kaspersky Endpoint Agent.
- Computers that are used for establishing remote connections to devices to scan those devices as part of security audit jobs.
- Computers hosting connector application modules.
- Computer hosting Kaspersky Security Center.
- Network switch.

Common deployment scenarios

Kaspersky Industrial CyberSecurity for Networks supports the following scenarios for installing components:

- Installing a Server without external sensors
- Installing a Server and external sensors

If necessary, a data diode can be used to connect a Server and/or sensors to an industrial network.

> Regardless of the installation method, it is recommended to use a special dedicated network for connecting Kaspersky Industrial CyberSecurity components (Kaspersky Industrial CyberSecurity for Networks, Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes, Kaspersky Security Center). The dedicated network's minimum bandwidth requirements for installation of the Kaspersky Industrial CyberSecurity for Networks Server and sensors are provided in the Hardware and software requirements article.

Installing a Server without external sensors

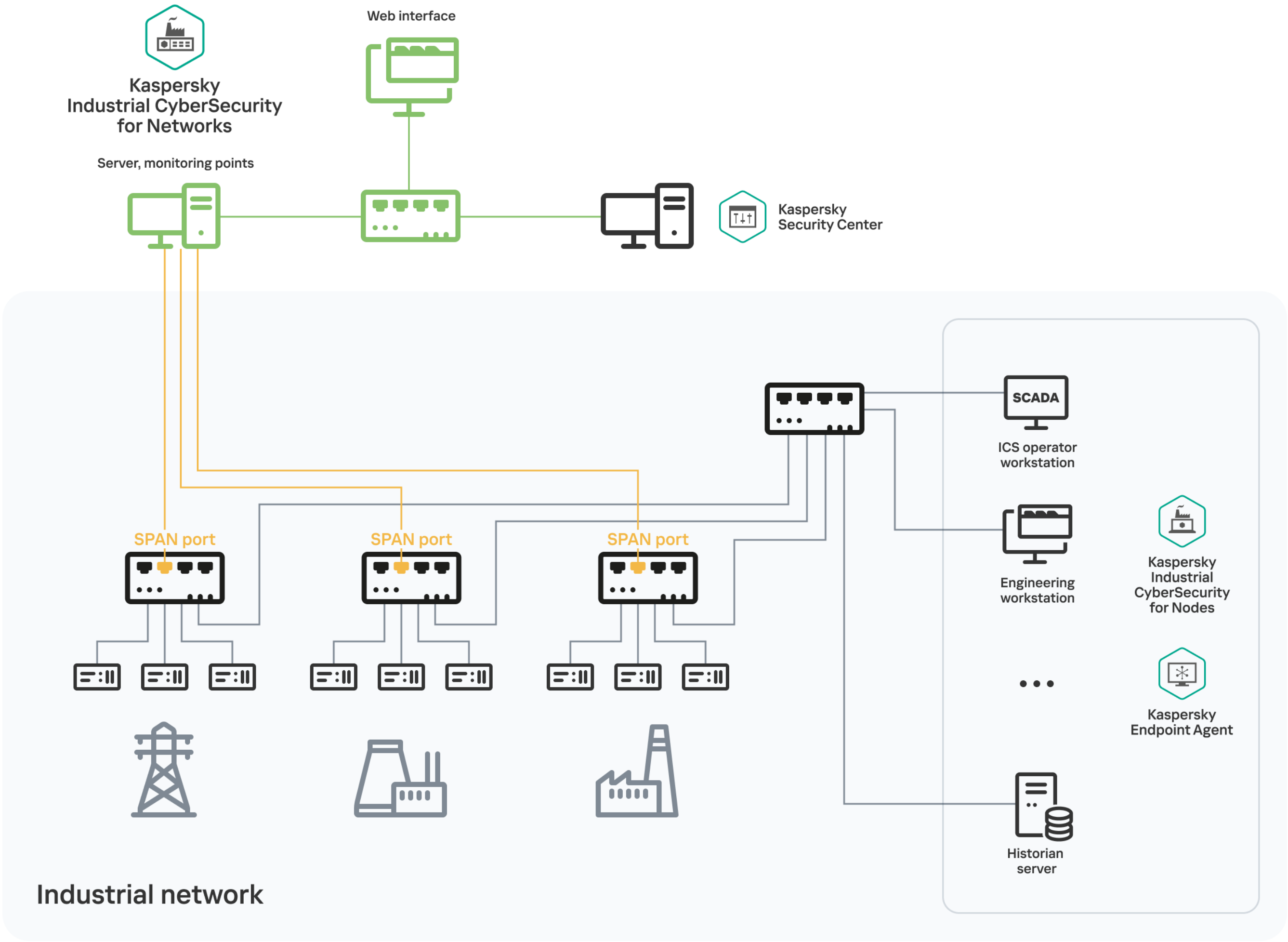
When installing a Server without external sensors, all data to be processed and analyzed is received only by the computer that performs Server functions. You can use this installation method if the computer has a sufficient number of network interfaces to receive data from various sources.

> If traffic aggregation tools (such as aggregation switches or network packet brokers) are used to transmit traffic to the Server in a distributed network architecture, the application may not be able to receive important data about the sources of information security events. In addition, if the same device addresses are used in different network segments, they cannot be processed correctly without additional configuration of traffic aggregation tools and the application. Moreover, individual network segments and devices may not be available for monitoring in the application, and the response and active polling functions may not be available for devices. For the most efficient operation of the application with traffic in a distributed network architecture, it is recommended to use the deployment scheme that involves the Server and external sensors.

The computer must have network interfaces to receive traffic on monitoring points from all industrial network segments. Due to the limit on the number of monitoring points on the Server, there must be no more than four of these network interfaces.

The computer must also have one more network interface so that other computers can connect to the Server through the web interface. There must be no monitoring points on this network interface. If there are no more free network interfaces on the computer, this same network interface can also be used for other connections from the dedicated Kaspersky Industrial CyberSecurity network.

The figure below shows an example scenario for deploying a Server without sensors. The network interfaces of the computer that performs Server functions are connected to the SPAN ports of network switches (SPAN ports and connections are marked yellow) and receive a copy of traffic from three segments of the industrial network. The dedicated Kaspersky Industrial CyberSecurity network is designated by green lines.



Example deployment of a Server without sensors

Installing a Server and external sensors

When installing a Server with external sensors, multiple computers can be used for installing application components. The Server is installed on one of the computers. The sensors that will receive data from computer networks are installed on the other computers. The application can have up to 50 sensors.

To receive traffic from the industrial network, you must add monitoring points to computers:

- No more than 8 monitoring points on a sensor
- No more than 4 monitoring points on the Server
- Total, no more than 50 monitoring points in the application

When using sensors in a network with a distributed network architecture, it is recommended to configure receiving all industrial network traffic at the sensor monitoring points, and not at the Server.

Monitoring points must be added to those network interfaces that will receive traffic from segments of the industrial network. A computer must have one network interface per each monitoring point.

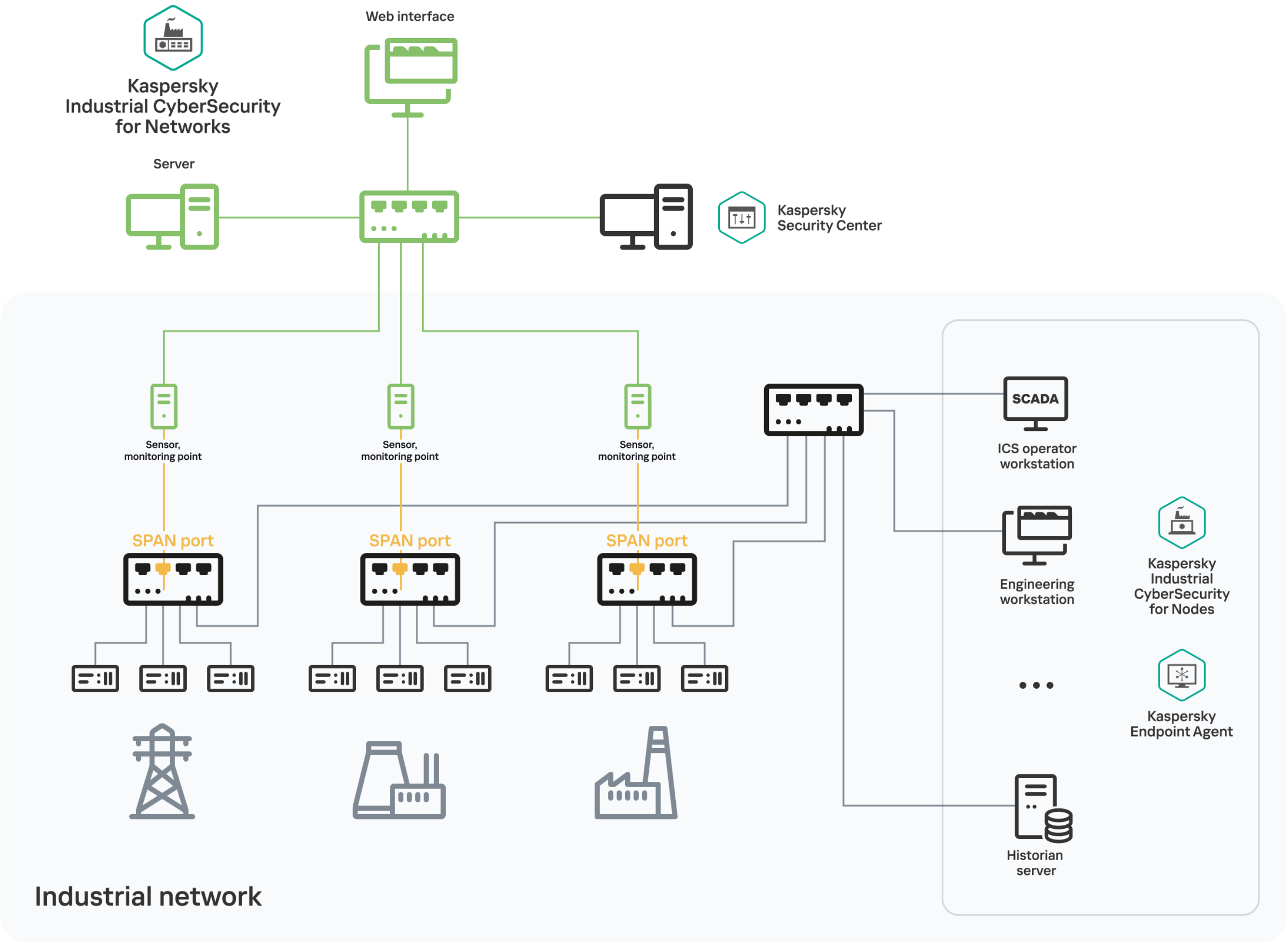
Computers must also have separate network interfaces that will be used for the following purposes:

- Connection with the Server (on computers that perform sensor functions)
- Connection with other computers through the web interface
- Other connections from the dedicated Kaspersky Industrial CyberSecurity network

For these purposes, each computer can use either multiple separate network interfaces or one shared network interface. There must be no monitoring points on these network interfaces.

> If you need to configure integration with Kaspersky Industrial CyberSecurity for Nodes and/or Kaspersky Industrial CyberSecurity for Linux Nodes installed in different network segments (for example, separated into industrial and corporate network segments), it is recommended to install sensors of Kaspersky Industrial CyberSecurity for Networks in the same segments where Kaspersky Industrial CyberSecurity for Nodes and/or Kaspersky Industrial CyberSecurity for Linux Nodes are installed. This configuration protects data transfer channels thanks to the interaction between the Server and sensors via a dedicated network, and does not require additional actions to configure access to devices and configure network segments.

The figure below shows an example scenario for deploying a Server and three sensors. The network interfaces of computers that perform sensor functions are connected to the SPAN ports of network switches (SPAN ports and connections are marked yellow) and receive a copy of traffic from their respective segments of the industrial network. The dedicated Kaspersky Industrial CyberSecurity network is designated by green lines.

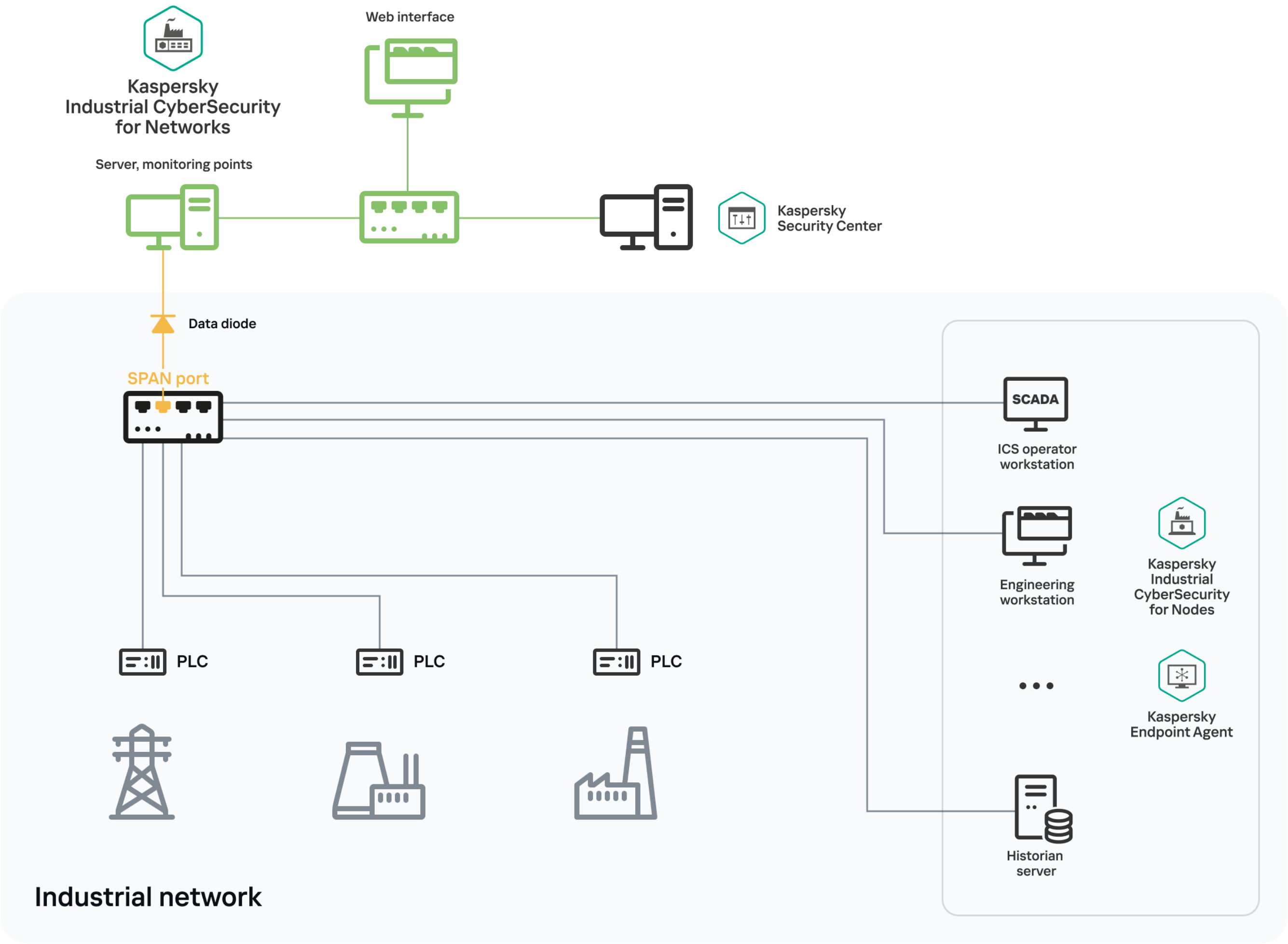


Example deployment of a Server and three sensors

Connecting Kaspersky Industrial CyberSecurity for Networks to an industrial network via data diode

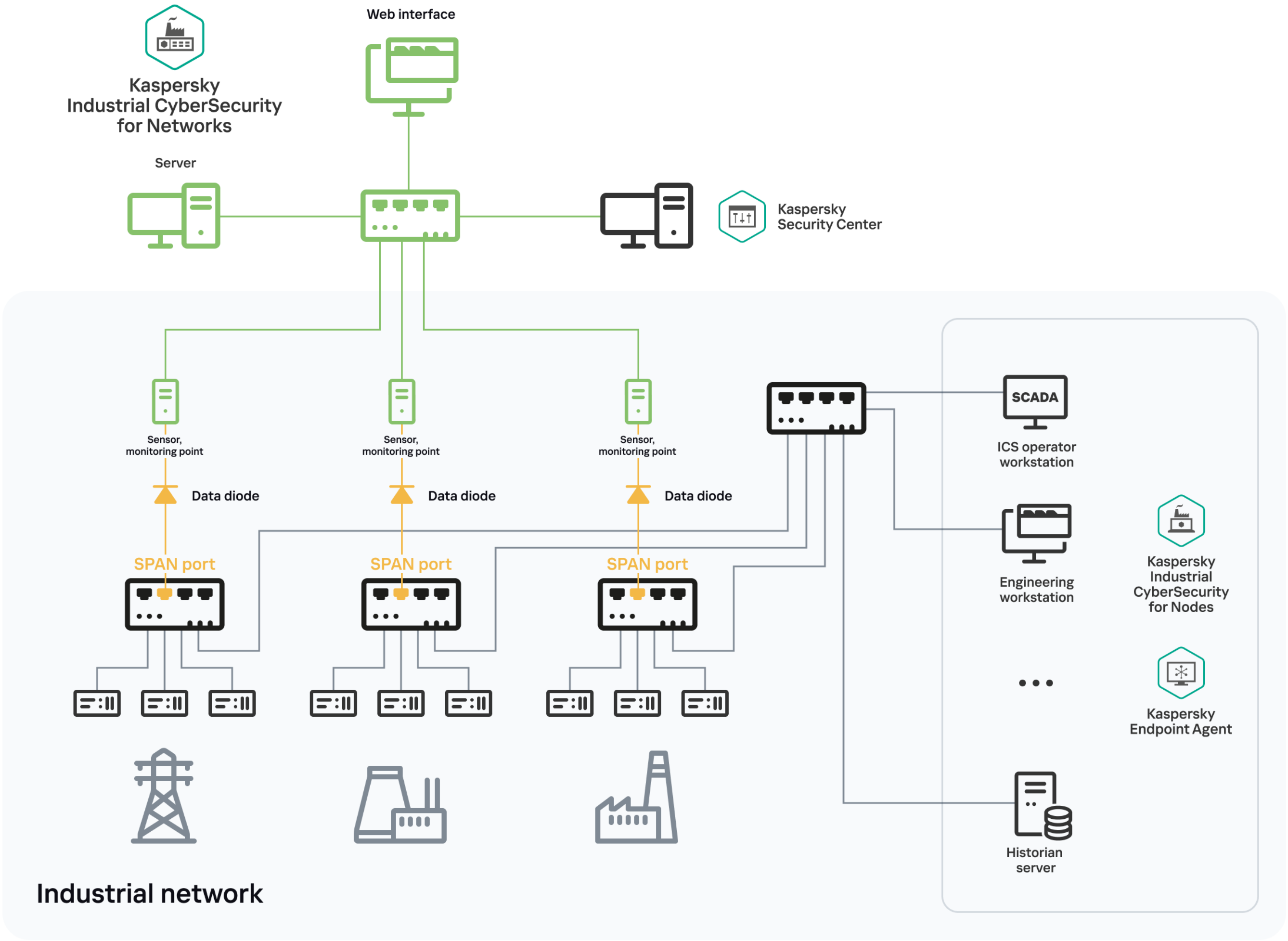
To connect Kaspersky Industrial CyberSecurity for Networks to an industrial network, you can additionally use special devices that provide unidirectional transmission of data from the industrial network. These devices are called *data diodes*. Data diodes can be installed on the connection links of monitoring points for Kaspersky Industrial CyberSecurity for Networks and on SPAN ports of network switches.

The figure below shows an example of connecting through a data diode to a monitoring point on the Server. In this deployment scenario, the Server is installed without external sensors.



Example Server connection via data diode

The example in the figure below shows the connection of multiple sensors of Kaspersky Industrial CyberSecurity for Networks via data diodes. In this deployment scenario, the Server is installed with three sensors.



Example connection of sensors via data diodes

Installing and removing the application

This section contains step-by-step instructions on installing and removing Kaspersky Industrial CyberSecurity for Networks.

Preparing for application installation

Before starting the installation of Kaspersky Industrial CyberSecurity for Networks, make sure that the computers meet the hardware and software requirements. Also make sure that the equipment, hardware, and software of the computers are compliant with all operational security recommendations.

> To ensure proper functioning of application components, it is recommended to use specially dedicated computers that only have software from the operating system installed. If third-party applications are installed on computers, the performance of components of Kaspersky Industrial CyberSecurity for Networks may be reduced.

To install application components, each computer must have a user account with root privileges that will be used to perform the installation. You can use the standard tools of the operating system to add the necessary user accounts.

Depending on the utilized application components installation script from the distribution kit, and on the type of application components being installed, you can do the following to prepare for application installation:

- **Preparing for centralized installation of components** ?

On the computers where components will be centrally installed, verify that the following conditions are fulfilled:

- The computers have network access, and access over SSH is configured and open.
- The computers have user accounts with root privileges (application components will be installed under these user accounts).
- The computers do not have any user accounts or groups with the following names that are reserved for interaction between application components (if these accounts exist, they could receive elevated access rights, even root privileges, after the application is installed):
  - kics4net
  - kics4net-apm
  - kics4net-asset-inventory
  - kics4net-blob-storage
  - kics4net-connectors
  - kics4net-connectors-launcher
  - kics4net-email-gateway
  - kics4net-epp-proxy
  - kics4net-fts
  - kics4net-nats-server
  - kics4net-oval-facade
  - kics4net-postgresql
  - kics4net-report-builder
  - kics4net-report-data-source
  - kics4net-report-renderer
  - kics4net-report-tc
  - kics4net-report-tcv
  - kics4net-responses-manager
  - kics4net-risk-oval-detector
  - kics4net-scap-manager
  - kics4net-scap-manager-view
  - kics4net-scan-oval-manager

- kics4net-scheduler
- kics4net-secrets
- kics4net-task-m
- kics4net-task-mv
- kics4net-vault
- kics4net-websensor
- kics4net-webserver

To prepare computers for installation of application components:

1. On all computers on which application components will be installed, set the same password for the user account with root privileges (application components will be installed under this user account). By default, the root user account is used to perform the installation. Memorize the user names and password. You will need to provide this data while the application installation script is running.

   > After application components are installed, you are advised to change the passwords for these users.

2. Find out and save the following information about the computers:
   - Name and IP address of the computer that will perform Server functions.
   - IP addresses of the computers that will perform sensor functions.
   - Name or IP address and SSL port of the computer with Kaspersky Security Center.

   To display the computer name, you can enter the `hostname` command in the command line. To display information about IP addresses and network interfaces, you can enter the `sudo ifconfig` command in the command line (in a Windows operating system, use the `ipconfig` command).

3. On the computer from which the centralized installation will be performed, use the SSH protocol to connect to each computer where the application components will be installed. A connection needs to be made to verify access over SSH.

   To connect:

   a. Enter the following command in the command line:

   ```
   ssh <user name >@< computer IP address >
   ```

   b. After entering this command, perform the necessary actions at the operating system prompts.

   c. To terminate the connection session, use the following command:

   ```
   exit
   ```

4. Copy the kics4net-release_<application version>.tar.gz archive from the distribution kit to the computer from which the installation will be performed.

5. Go to the folder containing the copied archive and enter the following command to unpack it:

```
tar -zxvf kics4net-release_< application version >.tar.gz
```

The unpacked folders and files will appear in the subfolder kics4net-release_<application version>.

- Preparing for local installation of the Server or a sensor

On the computer where the Server or sensor will be installed, verify that the following conditions are fulfilled:

- There is network access to the computer.
- The computer has a user account with root privileges (the local installation script will be run under this user account).
- The computer does not have any user accounts or groups with the following names that are reserved for interaction between application components (if these accounts exist, they could receive elevated access rights, even root privileges, after the application is installed):
  - If the Server will be installed:
    - kics4net
    - kics4net-apm
    - kics4net-asset-inventory
    - kics4net-blob-storage
    - kics4net-connectors
    - kics4net-connectors-launcher
    - kics4net-email-gateway
    - kics4net-epp-proxy
    - kics4net-fts
    - kics4net-nats-server
    - kics4net-oval-facade
    - kics4net-postgresql
    - kics4net-report-builder
    - kics4net-report-data-source
    - kics4net-report-renderer
    - kics4net-report-tc
    - kics4net-report-tcv
    - kics4net-responses-manager
    - kics4net-risk-oval-detector
    - kics4net-scap-manager
    - kics4net-scap-manager-view

    - kics4net-scan-oval-manager
    - kics4net-scheduler
    - kics4net-secrets
    - kics4net-task-m
    - kics4net-task-mv
    - kics4net-vault
    - kics4net-webserver
- If a sensor will be installed:
    - kics4net
    - kics4net-apm
    - kics4net-connectors
    - kics4net-connectors-launcher
    - kics4net-epp-proxy
    - kics4net-nats-server
    - kics4net-oval-facade
    - kics4net-websensor

To prepare the computer for the local installation of the Server or a sensor:

1. Find out and save the following information about the computer:

    - User account credentials for the account with root privileges that will be used to run the local installation script.
    - Name and IP address of the computer (for subsequent connection to this computer).

   To display the computer name, you can enter the `hostname` command in the command line. To display information about IP addresses and network interfaces, you can enter the `sudo ifconfig` command in the command line.

2. Copy the kics4net-release_<application version>.tar.gz archive from the distribution kit to the computer.

3. Go to the folder containing the copied archive and enter the following command to unpack it:

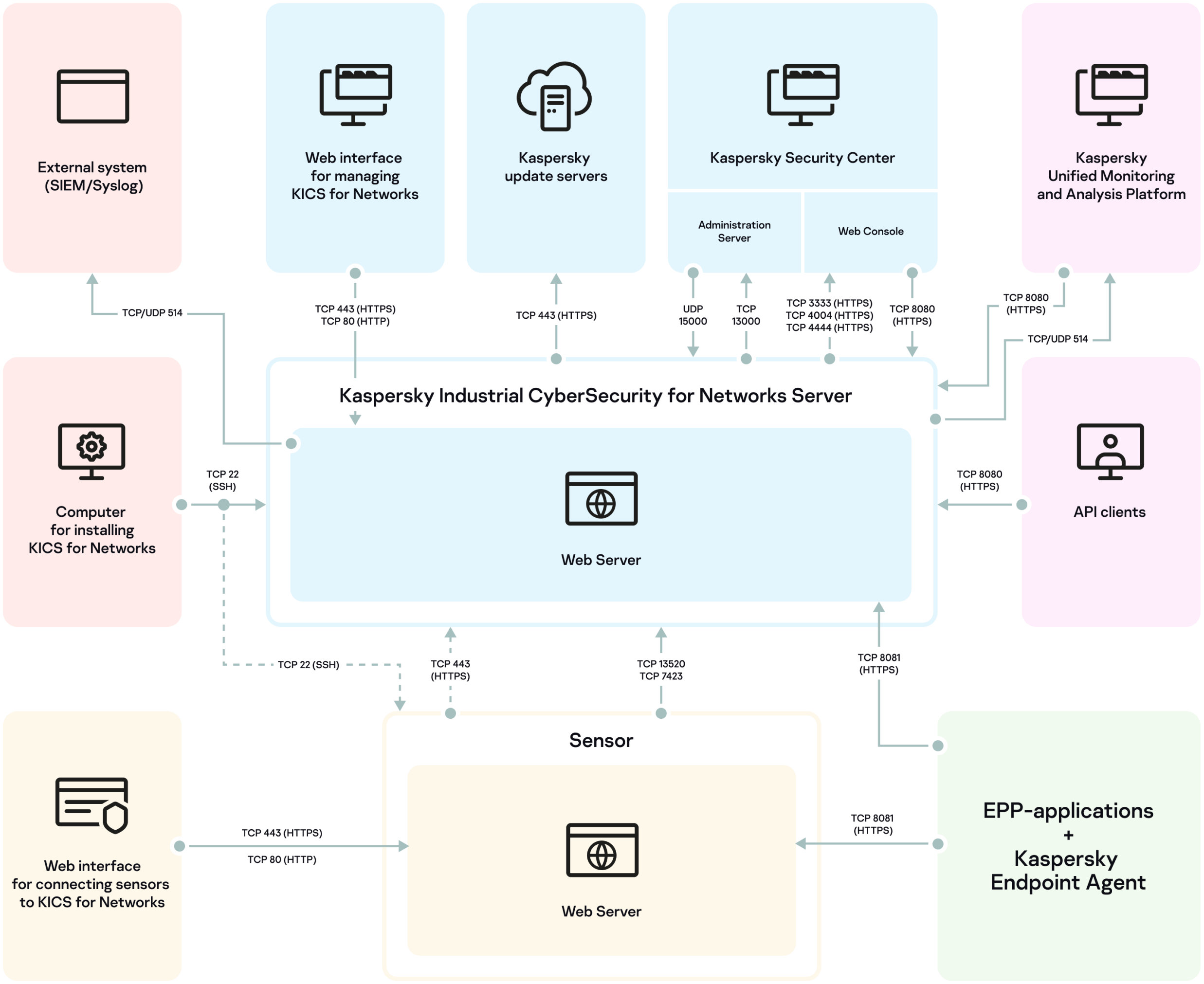
   ```
   tar -zxvf kics4net-release_< application version >.tar.gz
   ```

The unpacked folders and files will appear in the subfolder kics4net-release_<application version>.

Ports used for installation and operation of components

To ensure successful installation and operation of components of Kaspersky Industrial CyberSecurity for Networks, specific ports and protocols that will be used for data transfer must be available. You need to configure use of these ports and protocols in the settings of your network hardware or software that will be used to monitor network traffic.

The figure below shows the ports and protocols used by application components.



Utilized ports and protocols

The purpose of utilized ports is described in the table below.

Purpose of utilized ports

Port	Protocol	Description
Computer where application components are installed		
22	TCP (SSH)	This port is used to connect to nodes and to install Server and sensor components.
Computer that performs Server functions		

22	TCP (SSH)	This port is used for interaction with the computer where the application components are installed.
80	TCP (HTTP)	This port is used for connecting through the web interface.
443	TCP (HTTPS)	This port is used for the following purposes: • Connection through the web interface • Connection to Kaspersky update servers • Connection of a sensor through the web interface automatically over the network
514	TCP/UDP	This port is used to send data via SIEM and Syslog connectors.
3333 4004 4444	TCP (HTTPS)	Used for interaction with the Identity and Access Manager component in Kaspersky Security Center Web Console when using the single sign-on (SSO) technology.
7423	TCP	This port is used for connections of sensors.
8080	TCP (HTTPS)	This port is used for the following purposes: • Connection via the Kaspersky Industrial CyberSecurity for Networks API (including the KUMA connector) • Connecting Kaspersky Security Center Web Console
8081	TCP (HTTPS)	This port is used to receive data from EPP applications (if an integration server was added to the Server node).
13000	TCP	This port is used to connect Network Agent to the Kaspersky Security Center Administration Server.
13520	TCP	This port is used for connections of sensors.
15000	UDP	Used to send the control signals to the Network Agent from Kaspersky Security Center Administration Server.
Computer that performs sensor functions		
22	TCP (SSH)	This port is used for interaction with the computer where the application components are installed.
80	TCP (HTTP)	This port is used for connecting through the web interface.
8081	TCP (HTTPS)	This port is used to receive data from EPP applications (if an integration server was added to the sensor node).

Using a script for centralized installation of application components

This section provides information on the capabilities for using the application components centralized installation script kics4net-deploy-<application version number>.bundle.sh. You can use this script for centralized installation and removal of the Server and sensors of Kaspersky Industrial CyberSecurity for Networks.

If installation or removal of application components is performed using the kics4net-deploy-<application version number>.bundle.sh script, you are not required to apply the local installation or local removal scripts that are included in the application distribution kit.

Centralized installation of application components

This article describes the procedure for centralized installation of application components when using the script named kics4net-deploy-<application version number>.bundle.sh.

Prior to centrally installing components, you must perform the necessary actions to prepare for application installation.

The application components centralized installation script uses data that was saved in the installation settings file. Running the script does not require root privileges for the current user account on the computer from which the installation will be performed.

To centrally install components of Kaspersky Industrial CyberSecurity for Networks on computers:

1. On the computer from which the centralized installation will be performed, go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

2. Enter the command for running the application components centralized installation script:

   ```
   bash kics4net-deploy-< application version >.bundle.sh
   ```

   The screen prompts you to choose the language of the installation menu.

3. Select the language that you want to use in the installation menu.

   > The choice of the installation menu language does not affect the localization of the Kaspersky Industrial CyberSecurity for Networks components. The capability to choose the localization language of application components is available during initial configuration of Kaspersky Industrial CyberSecurity for Networks after a Server is installed.

4. In the menu for selecting the installation option, select **Run new installation**.

   The main centralized installation menu appears on the screen.

5. Perform the following actions:

   a. Click the **Add Server** menu item to add a Server node and configure the main settings for this node.

   b. If you want to configure additional settings for the Server node, select **Change Server settings** and configure the relevant settings.

   c. If the Server is installed with sensors, use the **Add sensor** menu item to add nodes of sensors.

   d. If you want to configure additional settings for added sensor nodes, select **Change sensor settings** and configure the relevant settings for each added node.

   e. Use the **Change the user running the installation** menu item to specify the user account with root privileges that will be used for centralized installation of application components. This user account will be used on those nodes for which no additional account was specified when configuring advanced settings.

6. When finished configuring the settings, select **Save settings and start installation**.

   You will be prompted to enter the password of the user running the installation.

7. Enter the password of the user running the installation. The password must be entered twice: first in the `SSH password` prompt and then in the `BECOME password` prompt.

   The installation script will begin the installation of components. During installation, the screen will display service messages regarding operations being completed.

   Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh.

After installation of Kaspersky Industrial CyberSecurity for Networks components is complete, the application is not yet ready to monitor your industrial network. To use the application, you need to perform the necessary actions to prepare the application for operation.

Centralized installation menu commands

This article provides information on the main commands in the centralized installation menu. The menu is displayed when you run the application components centralized installation script kics4net-deploy-<application version number>.bundle.sh. This file must be run in the folder that was created during preparations for application installation.

You can use the centralized installation menu to create or modify the application installation configuration and run the procedure for installing or removing components.

The installation menu has a hierarchical structure of items. The first level contains the items of the main menu. To select the necessary option, you must enter its number and press **ENTER**. If the selected item takes you to another group of items, a submenu will appear on the screen.

The menu items that define the values of settings may have default values or previously defined values. These values are displayed in brackets after the item name.

The main menu contains the following groups of commands:

- **Server installation management commands** ?

You can use the following installation menu commands to manage installation of the Server:

- **Add Server** – adds a new node that will be assigned Server functions. This item is available if the Server has not yet been added. If you select this option, you need to specify the main settings for the Server when the following prompts appear:
  - **Enter the IP address of the node for installation** – defines the IP address that will be used for connecting to the computer over the SSH protocol and installing the Server.
  - **Add the capability for application interaction with Kaspersky Security Center** – adds the functionality that allows use of the Kaspersky Security Center Administration Server to receive a license key and download updates, and to relay events and application state to Kaspersky Security Center. You do not have to add this functionality to relay events to other recipient systems.

    > If the capability for application interaction with Kaspersky Security Center has been added, the Network Agent component of Kaspersky Security Center is installed when the application is installed. Kaspersky Security Center Network Agent is not installed if this component is being used by another Kaspersky application (to avoid disrupting the interaction between this application and the Kaspersky Security Center Administration Server). In addition, the functionality for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center may be limited if the version of the installed Network Agent differs from the version of this component provided in the distribution kit of Kaspersky Industrial CyberSecurity for Networks.

  - **Enable time synchronization between Server and sensors** – enables automatic time synchronization between the Server and nodes on which sensors are installed.
- **Change Server settings** – modifies the settings of the added Server. You can use this menu item to change the main component settings that can be edited and to configure advanced settings. After selecting this item, you will see a submenu in which you can change the following settings:
  - **Specify an additional user to run the installation** – defines an additional user account that will be used to run the installation on the Server node. An additional user account needs to be specified if the user name with root privileges on this node differs from the user name defined in the **Change the user running the installation** item. The passwords of all user accounts that will be used to run the installation must match.
  - **Enable hardware Watchdog** – enables use of the hardware Watchdog. The *hardware Watchdog* is a hardware-implemented system for controlling system hangs. If a node has a hardware Watchdog, you can enable its use in Kaspersky Industrial CyberSecurity for Networks. If the use of a hardware Watchdog is enabled, specify its path in the **Specify path to hardware Watchdog** item.
  - **Disable hardware Watchdog** – disables use of the hardware Watchdog.
  - **Add the capability for application interaction with Kaspersky Security Center** – adds the functionality enabling the application to interact with Kaspersky Security Center (if this functionality was not already added). This menu item is analogous to the **Add the capability for application interaction with Kaspersky Security Center** item in the **Add Server** menu.
  - **Remove the capability for application interaction with Kaspersky Security Center** – removes the functionality that lets the application interact with Kaspersky Security Center.
  - **Enable time synchronization between Server and sensors** – enables automatic time synchronization between the Server and nodes if automatic synchronization was not already enabled. This menu item is equivalent to the **Enable time synchronization between Server and sensors** option in the **Add Server** menu.

  - **Disable time synchronization between Server and sensors** – disables automatic time synchronization between the Server and nodes.

  - **Create database again** – deletes the existing database and creates a new one during reinstallation of the application.

    > If you select this menu item, information in the existing database will be lost after Server installation.

- **Remove Server** – removes the Server node.

- Sensor installation management commands

  You can use the following installation menu commands to manage installation of sensors:

  - **Add sensor** – adds a new node that will be assigned sensor functions. If you select this option, you need to specify the main settings for the sensor when the **Enter the IP address of the node for installation** prompt appears. In this prompt, you can define the IP address that will be used for connecting to the computer over the SSH protocol and installing the sensor.

  - **Change sensor settings** – modifies the settings of the added sensor. You can use this menu item to change the main sensor settings that can be edited and to configure advanced settings. Selecting this menu item displays a list of nodes on which sensors have been added. After selecting a node, you will see a submenu in which you can change the following settings:

    - **Specify an additional user to run the installation** – defines an additional user account that will be used to run the centralized installation on the sensor node. An additional user account needs to be specified if the user name with root privileges on this node differs from the user name defined in the **Change the user running the installation** item. The passwords of all user accounts that will be used to run the installation must match.

    - **Enable hardware Watchdog** – enables use of the hardware Watchdog. The *hardware Watchdog* is a hardware-implemented system for controlling system hangs. If a node has a hardware Watchdog, you can enable its use in Kaspersky Industrial CyberSecurity for Networks. If the use of a hardware Watchdog is enabled, specify its path in the **Specify path to hardware Watchdog** item.

  - **Remove sensor** – removes the sensor node. Selecting this item displays a list of nodes on which sensors have been added.

- General installation commands

  General installation menu commands include the following commands:

  - **Change the user running the installation** – defines the user name with root privileges that runs the centralized installation of application components. The same password for the user accounts that will run the installation must be set on all computers. The password must be entered during installation of components.

  - **View application installation settings** – displays the list of installation settings and their values.

- Installation menu exit commands

You can use the following commands to exit the centralized installation menu:

- **Save settings and start installation** – install the Kaspersky Industrial CyberSecurity for Networks application components according to the defined installation settings. The defined settings are saved in the installation settings file. The application centralized installation script saves the installation settings file on each computer on which the script is run.
- **Save settings and exit without installing** – save changes to the installation settings file, terminate the application centralized installation script, and exit without installing components.
- **Exit without saving settings** – terminate the application centralized installation script without saving changes to the installation settings file.

Reconfiguration and centralized reinstallation of application components

You can centrally reinstall components of Kaspersky Industrial CyberSecurity for Networks. For example, reinstallation of components may be required in the following cases:

- To add a new sensor.
- To change settings that can be defined in the centralized installation menu.

To centrally reinstall application components, the script named kics4net-deploy-<application version number>.bundle.sh uses the installation settings file that was saved on the computer. If the installation settings file on this computer is corrupt or missing from its original folder, the application centralized installation script searches for a copy of the file on the computer and on other computers that have application components installed.

To centrally reinstall components of Kaspersky Industrial CyberSecurity for Networks:

1. Run the application centralized installation script by completing steps 1–3 of the installation procedure.
2. In the menu for selecting the installation option, select **Edit settings of current installation**.

   The main centralized installation menu appears on the screen.
3. Depending on the necessary result, perform the following actions:
   - Using the **Change Server settings** menu item, specify the necessary settings for the Server.

     You cannot change the IP address of the Server. If you want to change the IP address, you need to first remove the existing Server and then add it again with the new IP address by using the **Add Server** menu item (this menu item appears if a Server has not been added).
   - If the Server was installed with sensors, use the **Change sensor settings** menu item to specify the necessary settings for the sensors.

     You cannot change the IP address of a previously added sensor. If you want to change the IP address, you need to first remove the existing sensor and then add it again with the new IP address by using the **Add sensor** menu item. You can also use this menu item to add new sensors.
   - Use the **Change the user running the installation** menu item to specify the user name of the account with root privileges that will be used to centrally install the application components on computers. This account

will be used on those nodes for which no additional account was specified when configuring advanced settings of the Server or sensors.

4. When finished configuring the settings, select **Save settings and start installation**.

   You will be prompted to enter the password of the user running the installation.

5. Enter the password of the user running the installation. The password must be entered twice: first in the `SSH password` prompt and then in the `BECOME password` prompt.

   The installation script will begin the installation of components. During installation, the screen will display service messages regarding operations being completed.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh.

Centralized installation of application components in non-interactive mode

You can centrally install application components in non-interactive (silent) mode, which means without the interactive input of installation settings. For non-interactive centralized installation, you must use special settings when you run the application components centralized installation script kics4net-deploy-<application version number>.bundle.sh.

You must prepare an installation settings file for non-interactive centralized installation. You can prepare an installation settings file by using the script kics4net-deploy-<application version number>.bundle.sh.

To prepare a centralized installation settings file using the script:

1. Configure the centralized installation settings by completing steps 1–5 of the installation procedure.

2. Save the installation settings file by selecting the **Save settings and exit without installing** menu item.

   The installation settings file named inventory.json is saved in the /home/<user>/.config/kaspersky/kics4net-deploy/ folder (the application components will not be installed).

3. If necessary, copy the centralized installation settings file into a different folder.

After preparing the centralized installation settings file, you can centrally install the application components in non-interactive mode.

To centrally install application components in non-interactive mode:

1. On the computer from which the centralized installation will be performed, go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

2. Enter the following command:

   ```
   bash kics4net-deploy-< application version >.bundle.sh --silent-mode
   ```

   `silent-mode` enables non-interactive installation mode (mandatory parameter).

   In addition to the mandatory parameter, you may also add the following parameters for running the installation script:

   - `-i < path to the installation settings file >` indicates the full path and name of the centralized installation settings file. If the setting is not defined, the inventory.json file located in the /home/<user>/.config/kaspersky/kics4net-deploy/ folder is used.

- `--enable-debug-grpc-server` – installs a debug gRPC server. This gRPC server is used for testing purposes and is not required for normal use of the application.

  > If the script is run with the `--enable-debug-grpc-server` parameter, the application will lose its certified state.

  After you enter a script run command, the screen will prompt you to enter the password of the user running the centralized installation.

3. Enter the password of the user running the centralized installation. The password must be entered twice: first in the `SSH password` prompt and then in the `BECOME password` prompt.

   The centralized installation script will begin the installation of components. During installation, the screen will display service messages regarding operations being completed.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh.

Reinforcing the security of computers with application components installed

After installing Kaspersky Industrial CyberSecurity for Networks, it is recommended to reinforce the security of the operating systems on computers that have application components installed. To reinforce security, you can use the application components centralized installation script named kics4net-deploy-<application version number>.bundle.sh or locally run the kics4net-harden.sh script, which is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

You can use the script to perform the following actions:

- Enable prevention of the startup of operating system services that are not required for the operation of application components (for example, avahi-daemon and cups).

- Change the network configuration settings that impact the security of the operating system (for example, enable prevention of redirected network packet processing over the ICMP protocol).

The centralized application components installation script performs actions that harden the security on all computers that have application components installed.

> To reinforce security, this script uses the centralized installation settings file that was saved on the computer. If the centralized installation settings file on this computer is corrupt or missing from its original folder, the script searches for a copy of the file on the computer and on other computers that have application components installed.

To reinforce security of computers using the kics4net-deploy-<application version>.bundle.sh script:

1. On the computer from which the centralized installation performed, go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

2. Enter the following command:

   ```
   bash kics4net-deploy-< application version >.bundle.sh --harden < setting >
   ```

   where < `parameter` > is one of the following startup parameters:

- `-s` enables prevention of the startup of operating system services.

- `-n` modifies the network configuration settings.

- `-a` enables prevention of the startup of operating system services and modifies the network configuration settings.

3. In the `SSH password` and `BECOME password` prompts, enter the password for the user account that is running the centralized installation.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh. If it completes successfully, information is displayed about the actions performed on computers with application components installed.

Centralized removal of application components

Kaspersky Industrial CyberSecurity for Networks components can be removed centrally by using the kics4net-deploy-<application version number>.bundle.sh. This script lets you remove application components from individual nodes of the Server or sensors or fully uninstall the current version of the application as well as previous versions (beginning with version 2.0).

> For removal of components, the script kics4net-deploy-<application version number>.bundle.sh uses the centralized installation settings file that was saved on the computer. If the centralized installation settings file on this computer is corrupt or missing from its original folder, the application installation script searches for a copy of the file on the computer and on other computers that have application components installed.

To centrally remove application components from individual nodes:

1. Run the application components centralized installation script by completing steps 1–3 of the installation procedure.

2. In the menu for selecting the installation option, select **Edit settings of current installation**.

   The main centralized installation menu appears on the screen.

3. Depending on the necessary result, perform the following actions:

   - Use the **Remove Server** menu item to remove a Server node.

     > After removing the Server node, you need to add a different Server node to ensure proper performance of the application.

   - Use the **Remove sensor** menu item to remove a sensor node (if multiple sensors have been added to the application, select the relevant node in the list of nodes that have added sensors).

4. When finished configuring the settings, select **Save settings and start installation**.

5. In the `SSH password` and `BECOME password` prompts, enter the password for the user account that is performing the centralized removal of application components.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh.

To completely remove the application:

1. Run the application components centralized installation script by completing steps 1–3 of the installation procedure.
2. In the menu for selecting the installation option, select **Edit settings of current installation**.

   The main centralized installation menu appears on the screen.
3. Use the **Remove Server** menu item to remove a Server node.
4. If sensors have been added to the application, use the **Remove sensor** menu item to sequentially remove all nodes of sensors.
5. Use the **Removal settings** menu item to configure advanced settings for centralized removal. When this item is selected, the following prompts are displayed:
   - **Remove the application together with data**. If you want to delete all data saved by the application in the system, enter `y`. If you do not need to remove the data, enter `n`.
   - **Remove Network Agent**. If you want to remove the Kaspersky Security Center Network Agent component, enter `y`. If you do not need to remove this component, enter `n`. This prompt is displayed if an installed Network Agent is detected.
6. Select **Save settings and start installation**.
7. In the `SSH password` and `BECOME password` prompts, enter the password of the user account performing the centralized removal.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh.

Removal of Kaspersky Industrial CyberSecurity for Networks does not automatically delete the copied and unpacked files from the distribution kit. If necessary, these files can be manually deleted.

Using a script for local installation of application components

This article describes the procedure for local installation of an application component (Server or sensor) on a computer by using the kics4net-install.sh script.

Prior to locally installing components, you must perform the necessary actions to prepare for application installation.

The application components local installation script can install only one of the components (Server or sensor) on a computer. If an application component (for example, the Server) is already installed on a computer, you cannot install a different type of component (in this case, a sensor) on this computer. If you attempt to install the same type of component on the computer, the local installation script will reinstall the component.

When installing the Server, the Kaspersky Security Center Network Agent component is automatically installed. Kaspersky Security Center Network Agent is not installed if this component is being used by another Kaspersky application (to avoid disrupting the interaction between this application and the Kaspersky Security Center Administration Server). In addition, the functionality for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center may be limited if the version of the installed Network Agent differs from the version of this component provided in the distribution kit of Kaspersky Industrial CyberSecurity for Networks.

To locally install a Kaspersky Industrial CyberSecurity for Networks Server:

1. Log in to the system using the account credentials of a user account with root privileges that you want to use to run the local installation script.

2. Go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

3. Enter the command for running local installation of the Server:

   ```
   bash kics4net-install.sh --server
   ```

   where `server` is the setting for enabling Server installation mode (required setting).

   Additionally, you can specify the following parameter for running the installation script:

   `--enable-debug-grpc-server` – installs a debug gRPC server. This gRPC server is used for testing purposes and is not required for normal use of the application.

   > If the script is run with the `--enable-debug-grpc-server` parameter, the application will lose its certified state.

   The script will begin installation of the component. During installation, the screen will display service messages regarding operations being completed.

Please wait for the kics4net-install.sh script to finish.

To locally install a Kaspersky Industrial CyberSecurity for Networks sensor:

1. Log in to the system using the account credentials of a user account with root privileges that you want to use to run the local installation script.

2. Go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

3. Enter the command for starting local installation of a sensor:

   ```
   bash kics4net-install.sh --sensor
   ```

   where `sensor` is the setting for enabling sensor installation mode (required setting).

   The script will begin installation of the component. During installation, the screen will display service messages regarding operations being completed.

Please wait for the kics4net-install.sh script to finish.

Using a script for local removal of application components

This article describes the procedure for local removal of an application component (Server or sensor) from a computer by using the kics4net-remove.sh script.

To locally remove a component of Kaspersky Industrial CyberSecurity for Networks from a computer:

1. Log in to the system using the account credentials of a user account with root privileges that you want to use to run the local removal script.
2. Go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.
3. Enter the command for running the application components local removal script:
   - If you want to delete the installed component files and all data saved by the application in the system, enter the command:
     ```
     bash kics4net-remove.sh --full
     ```
   - If you only want to delete the installed component files, enter the command:
     ```
     bash kics4net-remove.sh
     ```

   The script will begin removal of the component. During removal, the screen will display service messages regarding operations being completed.

Wait for the kics4net-remove.sh script to finish.

Installing the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center

The administration plug-in for Kaspersky Industrial CyberSecurity for Networks allows you to use the functions of Kaspersky Security Center to work with Kaspersky Industrial CyberSecurity for Networks. Depending on the version of Kaspersky Security Center and the actions that you want to perform using Kaspersky Security Center, you can install the following management plug-ins:

- Management plug-in for Administration Console based on Microsoft Management Console (MMC) - this plug-in is intended for use in Kaspersky Security Center Windows.

  The management plug-in for the MMC-based Administration Console must be installed locally on the computer where the Kaspersky Security Center Administration Server is installed. To install, you need to use a file from the Kaspersky Industrial CyberSecurity for Networks kit. For a description of the provided plug-in installation procedures, please refer to this article.

- Web management plug-in for Kaspersky Security Center Web Console - this plug-in is intended for use in Kaspersky Security Center Linux, as well as for advanced centralized control and single sign-on technology in Kaspersky Security Center Windows.

  You can install and update the web management plug-in for Kaspersky Security Center Web Console in various ways that are available in the interface of Kaspersky Security Center Web Console.

Before installing the management plug-in for MMC-based Administration Console, copy the kics4net-sc-plugin_<plug-in version number>_<localization code>.msi file from the application distribution kit archive to the computer with the Administration Server installed. Run the file with the localization code that matches the localization language of Kaspersky Security Center. You can copy the file from the folder containing the unpacked files of the kics4net-release_<application version>.tar.gz archive to the computer on which the preparation for application installation will be performed. After unpacking the archive, the files for the installation of the administration plug-in are located in the kics4net-release_<application version>/sc_plugin subfolder.

You can install the management plug-in for the MMC-based Administration Console in one of the following ways:

- Using the Setup Wizard
- From the command line

The administration plug-in needs to be installed using an account that belongs to the group of local administrators.

To install the administration plug-in using the Wizard:

1. On the computer where the Kaspersky Security Center Administration Server is installed, run the file named kics4net-sc-plugin_<plug-in version number>_<localization code>.msi.

   After completing the preparatory actions, the plug-in installation wizard will start.

2. Follow the instructions of the Setup Wizard. When prompted to make changes by Windows User Account Control (UAC), click **Yes** and enter the local administrator credentials if necessary.

After the Installation Wizard finishes, the administration plug-in for Kaspersky Industrial CyberSecurity for Networks appears in the list of installed management plug-ins in the properties of the Kaspersky Security Center Administration Server (the Administration Server properties window in the MMC-based Administration Console, section **Advanced** → **Information about installed application management plug-ins**).

To install the administration plug-in from the command line:

1. On the computer where the Kaspersky Security Center Administration Server is installed, open the command line interface.

2. Go to the folder that contains the file named kics4net-sc-plugin_<plug-in version number>_<localization code>.msi.

3. Enter the following command in the command line:

   ```
   msiexec /package kics4net-sc-plugin_<plug-in version number>_<localization code>.msi
   ```

   After completing the preparatory actions, the plug-in installation wizard will start.

4. Follow the instructions of the Setup Wizard. When prompted to make changes by Windows User Account Control (UAC), click **Yes** and enter the local administrator credentials if necessary.

After the Installation Wizard finishes, the administration plug-in for Kaspersky Industrial CyberSecurity for Networks appears in the list of installed management plug-ins in the properties of the Kaspersky Security Center Administration Server (the Administration Server properties window in the MMC-based Administration Console, section **Advanced** → **Information about installed application management plug-ins**).

When working with the command line interface, you can use other standard plug-in installer startup parameters that are provided for Windows Installer. For example, if necessary, you can uninstall the management plug-in by using the corresponding startup option. To obtain information about the available startup parameters, enter the `kics4net-sc-plugin_<plug-in version number>_<localization code>.msi /help` command.

Updating using data migration script

You can upgrade a previous version of Kaspersky Industrial CyberSecurity for Networks using the kics4net-backup.sh data migration script from the distribution kit of the current application version. The capability to upgrade to the current version using the kics4net-backup.sh script is supported for application versions 4.0.0, and 4.0.1.

The kics4net-backup.sh script allows you to migrate the following data from the previous application version:

- Security policy
- Data on the state and/or operating modes of technologies and methods
- Settings for updating application modules and databases
- Information about an added license key
- Audit entries
- Application messages
- Vulnerability risks
- Registered events
- Saved traffic for events
- Network map data

In addition, the kics4net-backup.sh script allows you to save in the backup copy the following data about the node computer where the application component is installed:

- Configuration of application services
- Computer name
- Application version number

The kics4net-backup.sh script can be used to create a backup copy of the data and download the data from the backup copy locally on the computer where the script is running. Therefore, both to create a backup copy of data and to download the data from the backup copy, sequentially run the script on each computer with the application component installed. You can perform the steps for creating a backup copy of data and downloading the data from the backup copy in any order: you can first run the script on the Server computer and then on the sensor computers, or vice versa.

The scenario for upgrading from a previous version of the application using the kics4net-backup.sh script consists of the following steps:

1. **Creating a backup copy of data from the previous application version on the Server and sensors' computers**

   To create a backup copy of data from the previous application version, perform the following actions on each computer with the application components installed:

   1. On the computer with the previous version of the application components installed, copy the kics4net-release_<application version>.tar.gz archive from the application distribution kit into a directory of your choice.

   2. Go to the folder containing the copied archive and enter the following command to unpack it:

      ```
      tar -zxvf kics4net-release_< application version >.tar.gz
      ```

      The unpacked folders and files will appear in the subfolder kics4net-release_<application version>.

   3. Go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

   4. Run the kics4net-backup.sh script:

      - To create a backup copy of data on the Server computer, enter the following command:

        ```
        sudo bash kics4net-backup.sh -b -p < path to backup file > -e -t -n -f -d
        ```

      - To create a backup copy of data on the sensor computer, enter the following command:

        ```
        sudo bash kics4net-backup.sh -s -p < path to backup file > -e -t -n -f -d
        ```

      where:

      - `-b` is a setting that enables writing of the Server data to the backup file.
      - `-s` is a setting that enables logging sensor data to the backup file (mandatory setting when the sensor is running on the computer).
      - `-p` is a setting indicating the full path and name of the created backup file (required setting).
      - `-e` is a setting for disabling retention of registered events (events are saved by default).
      - `-t` is a setting for disabling retention of traffic (traffic is saved by default).
      - `-n` is a setting for disabling retention of network map data (network map data is saved by default).
      - `-f` is a setting for saving all available node data (the saved data can be downloaded from a backup copy only on the same node).
      - `-d` is a setting that stops the application services (if this setting is not specified, the application services are started after the script finishes).

      The script will begin the data backup process. Wait for the kics4net-backup.sh script to finish and save the backup file that is created.

2. **Removing the previous version of the application**

   This step is necessary if you want to install components of the current version of the application to the same nodes where components of the previous version are installed.

If a Server or sensor of the current version is installed on a separate computer (not on the node hosting a previous version of the component), copy the created backup file to this computer.

Components of a previous version of the application can be removed in the following ways:

- Centrally on all nodes where the previous version of the application was installed.

  This option uses the application components centralized installation script via the centralized removal procedure.

- Locally at each node where a component from the previous version of the application is installed.

  This option uses the application components local removal script (if a component from the previous version of the application provides the capability for local installation and local removal).

After removing components of the previous version of the application, make sure that the computers satisfy the hardware and software requirements for installing the current version. If necessary, install a supported operating system version and prepare the hardware and software on the computers.

3 Installing the current version of Kaspersky Industrial CyberSecurity for Networks and getting the application partially ready for use

At this step, you need to install components of the current version of Kaspersky Industrial CyberSecurity for Networks. To do so, you can perform the centralized installation procedure or install components by using the application components local installation script.

After installing components, you need to partially prepare the application for operation by completing steps 1–4 from the description of the preparation process.

> When adding monitoring points to the same network interfaces that were used in the previous version of the application, it is recommended to name the monitoring points the same as they were named in the previous version of the application. This will let you retain the link between events and the new monitoring points when you load data from the backup (otherwise, the names of old monitoring points will be marked as deleted in events if the same names are not found in the new version).

4 Loading data from the backup after installing the new version of the application

To download data from the created backup files, perform the following actions on each computer with the application components installed:

1. On the computer with the current version of the application component installed, go to the directory where the kics4net-backup.sh script is located. You can go to the same folder that you opened at step 1, or you can go to the folder /opt/kaspersky/kics4net/sbin/.

2. Run the kics4net-backup.sh script:

   - To download data from a backup copy on the Server computer, enter the following command:

     ```
     sudo bash kics4net-backup.sh -r -p <path to backup file> -f -d
     ```

   - To restore the previous version of the Server database, enter the following command:

     ```
     sudo bash kics4net-backup.sh --restore-database -p <path to backup file> -d
     ```

   - To download data from a backup copy on the sensor computer, enter the following command:

     ```
     sudo bash kics4net-backup.sh -l -p <path to backup file> -f -d
     ```

   where:

   - `-r` is a setting that enables reading and downloading of data from the Server backup file (mandatory setting when running on the Server computer).

- `-l` is a setting that enables reading and downloading of data from the sensor backup file (mandatory setting when running on the sensor computer).

- `-p` is a setting indicating the full path and name of the backup file (required setting).

- `-f` is a setting that restores all the saved node data (all data can be restored only when downloaded from a backup copy on the same node where this data was saved).

- `-d` is a setting that stops the application services (if this setting is not specified, the application services are started after the script finishes).

The script will begin to load data from the backup file into the application. Wait for the kics4net-backup.sh script to finish.

Installing an updated application version with a patch

Under certain conditions, Kaspersky experts may prepare updated application files with the applied *patches*. Patches are intended for adding or fixing the functionality of the current application version if such changes cannot be applied by updating the databases and application modules.

The updated application files with the applied patch (hereinafter also referred to as "updated application files") are supplied in the form of an archive similar to the archive included in the application distribution kit.

If the application components are not yet installed on the computers, you can use the archive with the updated application files to install the application, the same way as the archive from the distribution kit. To do so, when preparing for the application installation, unpack the archive with the updated application files, but not the archive from the distribution kit. You can perform all other actions to install the components in the same way as when using the archive from the distribution kit.

If the components of the current application version are already installed on the computers, to install the updated application files with the patch, use the patch installation script kics4net-install-patch.sh. The kics4net-install-patch.sh script allows you to replace the installed application components of the current version with application components of the updated version and to migrate the data accumulated by the current application version. If an error occurs when replacing the installed components, the script rolls back the installation of the updated application files and returns the application to the state it had when the script was run.

What data can be migrated from the current application version using the kics4net-install-patch.sh script

When replacing the installed application components of the current version with the application components of the updated version, the kics4net-install-patch.sh script allows you to transfer the following accumulated data:

- Security policy
- Data on the state and/or operating modes of technologies and methods
- Settings for updating application modules and databases
- Information about an added license key
- Audit entries
- Application messages
- Vulnerability risks
- Registered events
- Saved traffic for events
- Network map data
- Traffic dump files

The kics4net-install-patch.sh script is included in the application distribution kit and is in the archive with the updated application files.

The kics4net-install-patch.sh script installs the updated application files locally on the computer where the script is run. Therefore, to update all application components (Server and sensors), run the kics4net-install-patch.sh script sequentially on each computer with the installed application component. The components can be updated in any order: you can first update the application files on the Server computer and then on the sensor computers, or vice versa.

To install the updated application files on the computer where Kaspersky Industrial CyberSecurity for Networks Server or sensor is installed:

1. Prepare the directory to store the old files from the archive that was last used for installing components or for the last update of application files.

   If the directory with the old unpacked files already exists on the computer (for example, the directory was not deleted after the local installation of the component), you can use this directory for further actions. If there is no such directory, perform the following actions to prepare it:

   a. Copy the archive that was last used for installing the components or to update the application files to a directory of your choice.

   b. Go to the folder containing the copied archive and enter the following command to unpack it:

      ```
      tar -zxvf <archive file name>
      ```

      The unpacked directories and files appear in a subdirectory whose name matches the name of the archive file.

   In the description of the further actions, this prepared directory is referred to as a *directory with old files*.

2. Prepare the directory to store the new unpacked files from the received archive with the updated application files.

   To prepare the directory:

   a. Copy the archive containing the updated application files to your computer.

   b. Go to the folder containing the copied archive and enter the following command to unpack it:

      ```
      tar -zxvf <archive file name>
      ```

      The unpacked directories and files appear in a subdirectory whose name matches the name of the archive file.

   In the description of the further actions, this prepared directory is referred to as a *directory with new files*.

3. In the directory with the new files, go to the <archive file name>/linux-centos subdirectory. This directory contains files of scripts and packages for installing, verifying and removing application components.

4. Run the kics4net-install-patch.sh script:

   - To install the updated application files on the Server computer, enter the following command:

     ```
     sudo bash kics4net-install-patch.sh -o <path to the directory with the old
     files>/linux-centos -n <path to the directory with the new files>/linux-centos -b
     <path to the directory with the backup copy> --backup-traffic
     ```

   - To install the updated application files on the sensor computer, enter the following command:

     ```
     sudo bash kics4net-install-patch.sh -s -o <path to the directory with the old
     files>/linux-centos -n <path to the directory with the new files>/linux-centos -b
     <path to the directory with the backup copy> --backup-traffic
     ```

   where:

   - `-o` is a parameter specifying the full path to the directory that contains the scripts and package files for installation, verification, and removal of the application components in the directory with the old files (mandatory parameter).

   - `- n` is a parameter specifying the full path to the directory that contains the scripts and package files for installation, verification, and removal of the application components in the directory with the new files (mandatory parameter).

   - `-b` is a parameter specifying the full path to the directory for creating the backup copy (by default, the script creates a backup copy in a temporary directory and automatically deletes the created files if the installation of the updated application files is successful or if the installation is rolled back due to an error during the script operation).

     > It is recommended to use this parameter to save the backup copy in the correct directory regardless of the kics4net-install-patch.sh script execution results. If a large amount of data is accumulated in the application, use the `-b` parameter to specify a mounted directory on a different hard drive and avoid the overflowing of the system (root) partition.

   - `--backup-traffic` is a parameter for adding the traffic dump files to the backup and further restoring these files after the updated application files are installed. By default, the traffic dump files are not copied to the backup directory; these files remain in their original location and are available if the installation is successful. This parameter allows you to automatically restore the traffic dump files in case of the rollback of the updated application files installation caused by an error in the kics4net-install-patch.sh script execution.

> It is recommended to use this parameter if you want to save the traffic dump files and there is a risk of errors during the installation of the updated application files. Typically, the directory where the application stores the traffic dump files requires a large amount of disk space. When the `--backup-traffic` parameter is used, the kics4net-install-patch.sh script copies these files to the backup directory, which may require significant additional disk space. Also, the script running time may significantly increase.

- `-s` is a parameter for enabling installation of the updated sensor files; it is applied when the kics4net-install-patch.sh script is run on the sensor computer.

  Example:

  ```
  sudo bash kics4net-install-patch.sh -o /tmp/kics4net-release_< application version number >/linux-centos -n
  /tmp/kics4net-patch1_< application version number >/linux-centos -b ./old_kics4net_data --backup-traffic
  ```

The script starts installing the updated application files. Wait for the kics4net-install-patch.sh script to finish.

To view the application version on the Server and start working with the application after installing the updated files:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. Use the IP address of the Server computer for the connection.

2. Select the **About** section and view the version of the application installed on the Server.

3. Select **Initial configuration**.

4. Please read the terms of the End User License Agreement and the Privacy Policy. To do so, open each document by using the corresponding links in the names of the following check boxes: **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.

5. If you fully agree to the terms of the End User License Agreement and the Privacy Policy, select both check boxes.

   > If you do not agree to the terms of the End User License Agreement and/or the Privacy Policy, close the web interface page and remove the installed application components from your computers.

6. Click the **Continue** button.

Getting started

After installing components of Kaspersky Industrial CyberSecurity for Networks, you need to prepare the application for operation. The preparation process consists of the following main steps:

1. Initial configuration of the application

   At this step, the main application settings are configured after Server installation. After this step is completed, the Server will be available for connection and for operations with the application through the web interface.

2. Adding and connecting sensors

This step is necessary when you install external sensors along with the Server. After this step is completed, nodes that have sensors installed will be ready for further configuration.

3. **Adding monitoring points**

   At this step, monitoring points are added on nodes that have application components installed. After this step is completed, the application begins to analyze traffic coming from industrial network segments to network interfaces hosting monitoring points.

4. **Adding application users**

   At this step, application user accounts are created in addition to the user account that was created during initial configuration of the application. After this step is completed, the application will have multiple user accounts that you can use to restrict access to application functions and monitor activity based on audit entries.

5. **Adding a license key**

   This step adds a license key to the application to activate the corresponding application functionality. After this step is completed, you will be able to configure and utilize the functionality for updating application modules and databases. Also, if the license key enables the active device polling functionality, you will be able to do that too.

6. **Configuring updates of application modules and databases**

   This step is necessary if a license key was added to the application. After this step is completed, you will be able to install updates for application modules and databases.

7. **Configuring Asset Management**

   At this step, lists of known devices are generated. In some cases, you may have to configure address spaces. To obtain the most accurate and complete information about devices and their configurations, you can conduct active polling of devices. After this step is completed, the application will be configured to track the relevant devices in the industrial network.

8. **Configuring Process Control**

   At this step, the settings of devices are configured for proper industrial process control by the application. After this step is completed, you will be able to use the application to monitor industrial process parameters (including with the use of rules) and track the system commands that are transmitted.

9. **Configuring Interaction Control**

   At this step, rules are generated to identify network interactions that are authorized or unauthorized by the application. After this step is completed, rules allowing interactions between specific devices and authorized system commands will be configured (the application will not register events when these rules are triggered).

10. **Configuring Intrusion Detection**

    This step is necessary for configuring the application to implement Intrusion Detection functionality. After this step is completed, you will be able to use Intrusion Detection rules (already embedded rules and/or rules additionally uploaded to the application) and track traffic anomalies showing signs of an attack.

11. **Configuring device security audit**

    This step is performed for the security audit of monitored devices using Kaspersky Industrial CyberSecurity for Networks. Once this step is performed, the application can assess device compliance with security standards and perform other checks using security audit jobs.

Initial configuration of the application after Server installation

After the Server is installed using the script for centralized installation or another method, the application awaits completion of initial configuration. Initial configuration can be completed by any user connected to the Server through the web interface.

To perform initial configuration of the application after a Server is installed:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. Use the IP address of the Server computer for the connection.

2. Select **Initial configuration**.

3. In the **Application localization language** field, select the localization language for components of Kaspersky Industrial CyberSecurity for Networks (and for the data provided by these components).

4. In the **Administrator account** settings group, define the user account name and password for the first application user. The Administrator role will be assigned to this user. This user does not have to be registered as an operating system account on the Server computer or other computer.

   For the account name, you can enter any unique name using uppercase and lowercase letters of the English alphabet, numerals, dots, and the following special characters: _ and - (for example, Admin_1). The name must contain from 3 to 20 characters, must begin with a letter, and end with any supported character except a dot.

   The password must meet the following requirements:

   - Must contain between 8 and 256 ASCII characters.

   - Must contain one or more uppercase letters of the English alphabet.

   - Must contain one or more lowercase letters of the Latin alphabet.

   - Must contain one or more numerals.

   - Must contain no more than three consecutive repeated characters.

5. In the **Application Server** field, enter the name of the Server used in Kaspersky Industrial CyberSecurity.

   The Server name must be unique (not match the names of sensors on other nodes) and must contain no more than 100 characters. You can use letters of the English alphabet, numerals, a space, and the following special characters: `_` and `-` (for example, `Server_1`). The Server name must begin and end with any permitted character except a space.

6. Please read the terms of the End User License Agreement and the Privacy Policy. To do so, open each document by using the corresponding links in the names of the following check boxes: **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.

7. If you fully agree to the terms of the End User License Agreement and the Privacy Policy, select both check boxes.

   > If you do not agree to the terms of the End User License Agreement and/or the Privacy Policy, close the web interface page and remove the installed application components from your computers.

8. Click the **Continue** button.

After the defined settings are applied, the web interface page will open to the normal operating mode of the application. The account credentials of the first application user will be used for the current connection session.

You can revert the Server to the initial state using the kics4net-reset-to-defaults.sh script. The script is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

Starting and stopping the application

A component of the application installed on a computer is started automatically when the operating system of the computer is loaded. An application component must be configured so that it can work properly. Components are configured when the application is being prepared for operation.

The application performs industrial network traffic analysis functions if it receives traffic through monitoring points. You can disable or enable monitoring points to suspend or resume analysis of traffic received by these monitoring points.

Nodes with Kaspersky Industrial CyberSecurity for Networks components installed receive and process data from EPP applications if integration servers were added on these nodes. You can disable and enable integration servers to suspend and resume receipt of data from EPP applications, respectively.

The application lets you conduct active polling of devices. Active polls are performed by using connectors, which let you obtain various information about devices, including for the generation of a topology map. You can enable and disable connectors to pause and resume the sending and receiving of data through those connectors.

To manage operation of the application and view information, you can connect to the Server through the web interface. When you are done working with the Server, you are advised to properly terminate the connection session.

To configure the connection between a sensor and the Server, and to view information about the connection state, you can connect to the sensor through the web interface. When connecting to a sensor, you are not required to enter your user account credentials. Therefore, you do not need to do anything to terminate the connection session.

Connecting to the Server through the web interface

You can use any supported browser to connect to the Server through the web interface. You can connect from any computer that has network access to the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server.

To connect to the Kaspersky Industrial CyberSecurity for Networks Server:

1. Open your browser and enter the following in the address bar:
   ```
   https://<Server name>:<port>
   ```
   where:

   - `<Server name>` is the IP address or computer name used by the web server on the Server computer.
   - `<port>` is the port number specified for the web server.

   > If a port number is not specified (prior to initial configuration of the application) or if the default port number (443) is specified for the web server, you only need to enter the IP address or computer name of the Server in the address bar. In this case, the HTTPS protocol and the port number will be automatically determined.

2. When the account credentials entry page opens, enter the application user name and password and click the **Log in** button.

The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens in the browser window. The name of the browser bookmark for the web interface page will show the Server name that was defined during initial configuration of the application after installation.

A Server connection session has a time limit. A session remains active for 10 hours. If 10 hours have passed since the connection was established, the current page of the application web interface switches to the page for entering account credentials. If this happens, to continue working you will need to re-enter your application user name and password.

Terminating a Server connection session through the web interface

When you finished working with the Kaspersky Industrial CyberSecurity for Networks Server using the web interface, make sure you close the connection session in your browser.

If you close the browser window without first finishing the connection session, the session will remain active. A session remains active for 10 hours. During this time, the application can grant access to the web interface of the Kaspersky Industrial CyberSecurity for Networks Server without prompting for user account credentials, provided that the connection is used by the same computer, browser, and operating system account.

To close the connection session with the Kaspersky Industrial CyberSecurity for Networks Server:

1. On the Kaspersky Industrial CyberSecurity for Networks Server web interface page, open the user menu:
   - If the menu is collapsed, click the 👤 button.
   - If the menu is expanded, click the button on the right of the name of the current user.
2. In the user menu, select **Log out**.

   The browser window shows the page for entering account credentials.

Connecting to a sensor through the web interface

When you are connected to a sensor via the web interface, the following actions are available on the sensor web interface page:

- Download a communication data package to the sensor for connecting to the Kaspersky Industrial CyberSecurity for Networks Server.
- View the fingerprint of the certificate signing request to compare it with the fingerprint on the Server web interface page if the sensor is being connected to the Server automatically over the network.
- View information about the status of the connection between the sensor and the Server.

To change sensor settings, manage monitoring points and technologies, and monitor the status of the node, connect to the application Server via the web interface.

You can use any supported browser for connecting to the Sensor via the web interface. This connection can be established from a computer that can access the sensor computer over the network.

To connect to a Kaspersky Industrial CyberSecurity for Networks sensor:

Open your browser and enter the following into the address bar:
`https://<sensor name>:<port>`

where:

- `<sensor name>` is the IP address or name of the sensor computer used by the web server of the sensor.
- `<port>` is the port number used by the web server of the sensor.

> If the default port number (443) is used for the sensor web server, you only need to enter the IP address or computer name of the sensor into the address bar. In this case, the HTTPS protocol and the port number will be automatically determined.

The Kaspersky Industrial CyberSecurity for Networks sensor web interface page opens in the browser window. The browser tab for the web interface page displays the sensor name defined when it was added.

Application interface

This section describes the primary application interface elements.

Kaspersky Industrial CyberSecurity for Networks Server web interface

When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface, the Server web interface page opens in your browser. The contents of the web interface page depend on the application operating mode and on the specific role of the connected user account.

Depending on the application operating mode, the web interface page may contain the following management elements or messages:

- Initial configuration of the application – management elements for configuring the Server after its installation and for viewing and accepting the End User License Agreement and Privacy Policy.
- Normal operating mode of the application – management elements for configuring and utilizing application functionality.
- Application maintenance – message regarding an operation that must be completed before the Server will be available for connections.

When the application is running in its normal operating mode, its available functionality on the web interface page depends on the role of the connected user account. If the user role does not grant the permissions to utilize application management functions, the corresponding management elements are either not displayed on the web interface page or are unavailable.

About the Server web interface during initial configuration of the application

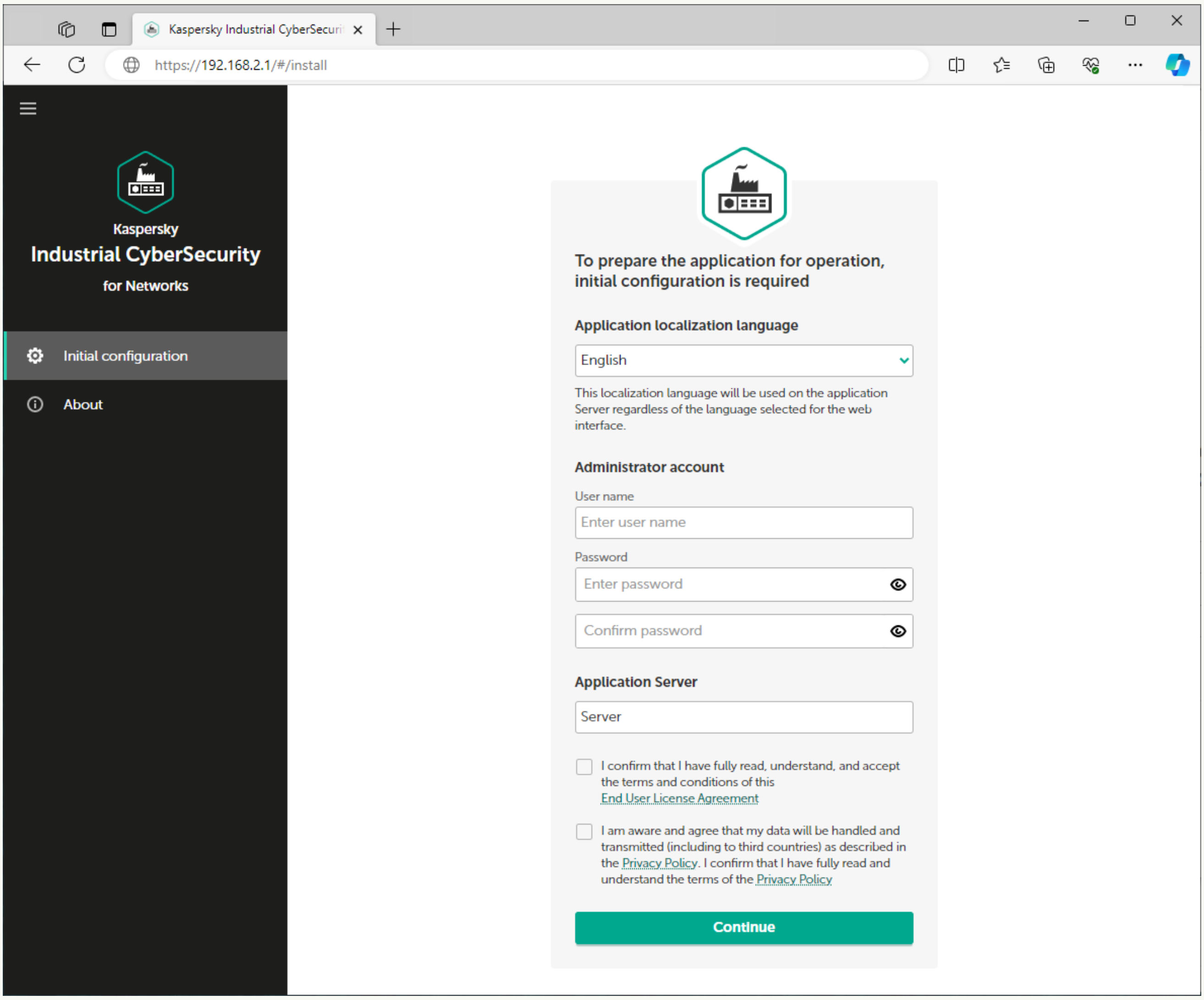
When connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface for the first time after installing the application, you are not prompted to enter your user account credentials to log in. Instead of the account credentials entry page, you see a page containing management elements for configuring the Server and for viewing and accepting the End User License Agreement and Privacy Policy.

A menu is displayed in the left part of the web interface page. The contents of the selected section are displayed on the right.

The web interface menu contains the following items:

- ☰ – expands and collapses the menu. If the menu is collapsed, the items are displayed without text descriptions.
- ⚙ – opens the **Initial configuration** section.

In the **Initial configuration** section of the Server web interface (see the figure below), you can configure the Application Server's main settings that are required before the application can begin operations after installation.



To prepare the application for operation, initial configuration is required

Application localization language

English

This localization language will be used on the application Server regardless of the language selected for the web interface.

Administrator account

User name

Enter user name

Password

Enter password

Confirm password

Application Server

Server

□ I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement

□ I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy

Continue

Initial configuration section

This section contains a window that you can use to configure the main settings of the Server, create the first user with the Administrator role, and carefully read and accept the terms of the End User License Agreement and Privacy Policy. After completing these actions, this web interface page will automatically close (along with other Server connection sessions through the web interface) and you will be taken to the Server web interface page for the normal operating mode of the application.

- ⓘ – opens a section containing brief information about the application.

About the Server web interface during normal operation of the application

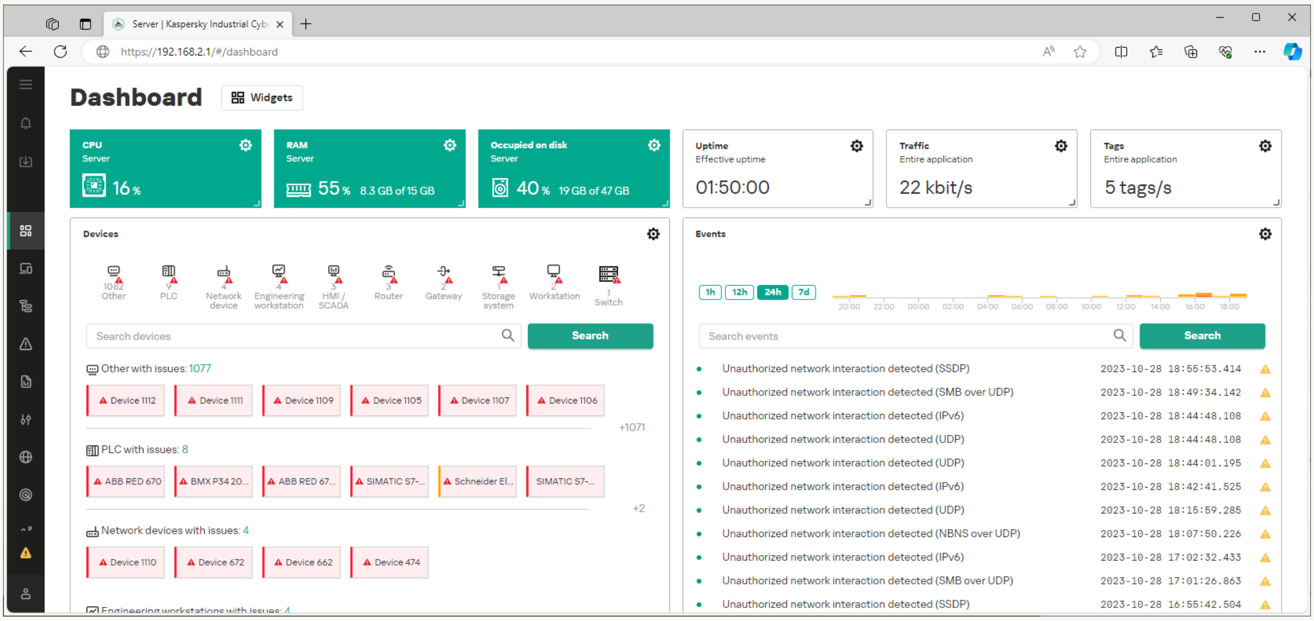
After connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface while the application is running in normal operating mode, a web interface page opens to provide tools for working with the application. The available tools and their functionality depend on the role of the user who established the connection to the Server.

A menu is displayed in the left part of the web interface page. The contents of the selected section are displayed on the right.

The web interface menu contains the following items:

- ☰ – expands and collapses the menu. If the menu is collapsed, the items are displayed without text descriptions.
- 🔔 – opens a list of notifications regarding application operating issues. The availability of notifications is indicated by an icon whose color corresponds to the status of the notifications.
- ⤓ – opens a list of background operations. This list contains information about operations that take a long time (for example, creating a file when exporting a large number of events). The number of active background operations and their progress status are indicated by an icon. The icon is colored red if there are operations that resulted in errors.
- ⊞ – opens the Dashboard section.

In the **Dashboard** section of the Application Server web interface (see the figure below), you can view information about the current state of the system in online mode.



CPU
Server
16 %

RAM
Server
55 % 8.3 GB of 15 GB

Occupied on disk
Server
40 % 19 GB of 47 GB

Uptime
Effective uptime
01:50:00

Traffic
Entire application
22 kbit/s

Tags
Entire application
5 tags/s

1082 Other · 9 PLC · 4 Network device · 4 Engineering workstation · 3 HMI / SCADA · 3 Router · 2 Gateway · 1 Storage system · 2 Workstation · 1 Switch

Other with issues: 1077

Device 1112 · Device 1111 · Device 1109 · Device 1105 · Device 1107 · Device 1106 · +1071

PLC with issues: 8

ABB RED 670 · BMX P34 20... · ABB RED 67... · SIMATIC S7-... · Schneider El... · SIMATIC S7-... · +2

Network devices with issues: 4

Device 1110 · Device 672 · Device 662 · Device 474

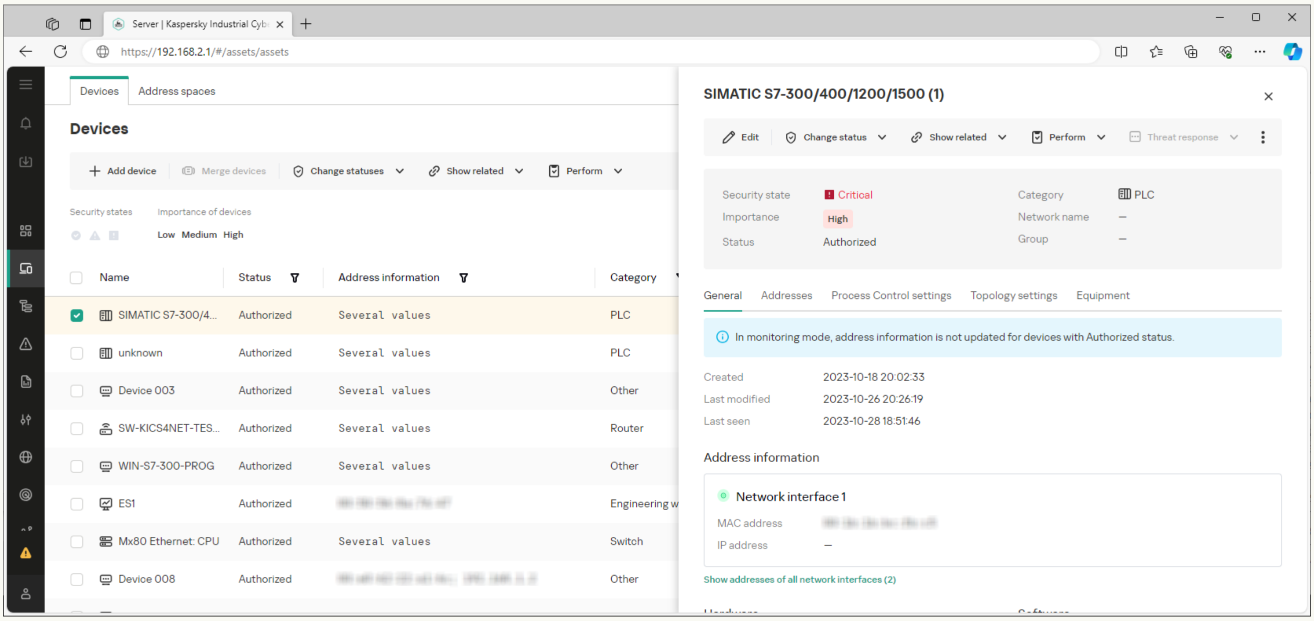
Engineering workstations with issues: 4

```
Unauthorized network interaction detected (SSDP)            2023-10-28 18:55:53.414
Unauthorized network interaction detected (SMB over UDP)    2023-10-28 18:49:34.142
Unauthorized network interaction detected (IPv6)            2023-10-28 18:44:48.108
Unauthorized network interaction detected (UDP)             2023-10-28 18:44:48.108
Unauthorized network interaction detected (UDP)             2023-10-28 18:44:01.195
Unauthorized network interaction detected (IPv6)            2023-10-28 18:42:41.525
Unauthorized network interaction detected (UDP)             2023-10-28 18:15:59.285
Unauthorized network interaction detected (NBNS over UDP)   2023-10-28 18:07:50.226
Unauthorized network interaction detected (IPv6)            2023-10-28 17:02:32.433
Unauthorized network interaction detected (SMB over UDP)    2023-10-28 17:01:26.863
Unauthorized network interaction detected (SSDP)            2023-10-28 16:55:42.504
```

Dashboard section

- ⧉ – opens the Assets section.

In the **Assets** section of the Application Server web interface (see the figure below), you can view and edit information about devices and device address space settings.



Devices

Name	Status	Address information	Category
☑ SIMATIC S7-300/4...	Authorized	Several values	PLC
□ unknown	Authorized	Several values	PLC
□ Device 003	Authorized	Several values	Other
□ SW-KICS4NET-TES...	Authorized	Several values	Router
□ WIN-S7-300-PROG	Authorized	Several values	Other
□ ES1	Authorized	[redacted]	Engineering w
□ Mx80 Ethernet: CPU	Authorized	Several values	Switch
□ Device 008	Authorized	[redacted]	Other

SIMATIC S7-300/400/1200/1500 (1)

Security state	Critical	Category	PLC
Importance	High	Network name	—
Status	Authorized	Group	—

In monitoring mode, address information is not updated for devices with Authorized status.

Created	2023-10-18 20:02:33
Last modified	2023-10-26 20:26:19
Last seen	2023-10-28 18:51:46

Address information

Network interface 1

MAC address [redacted]

IP address —

Show addresses of all network interfaces (2)

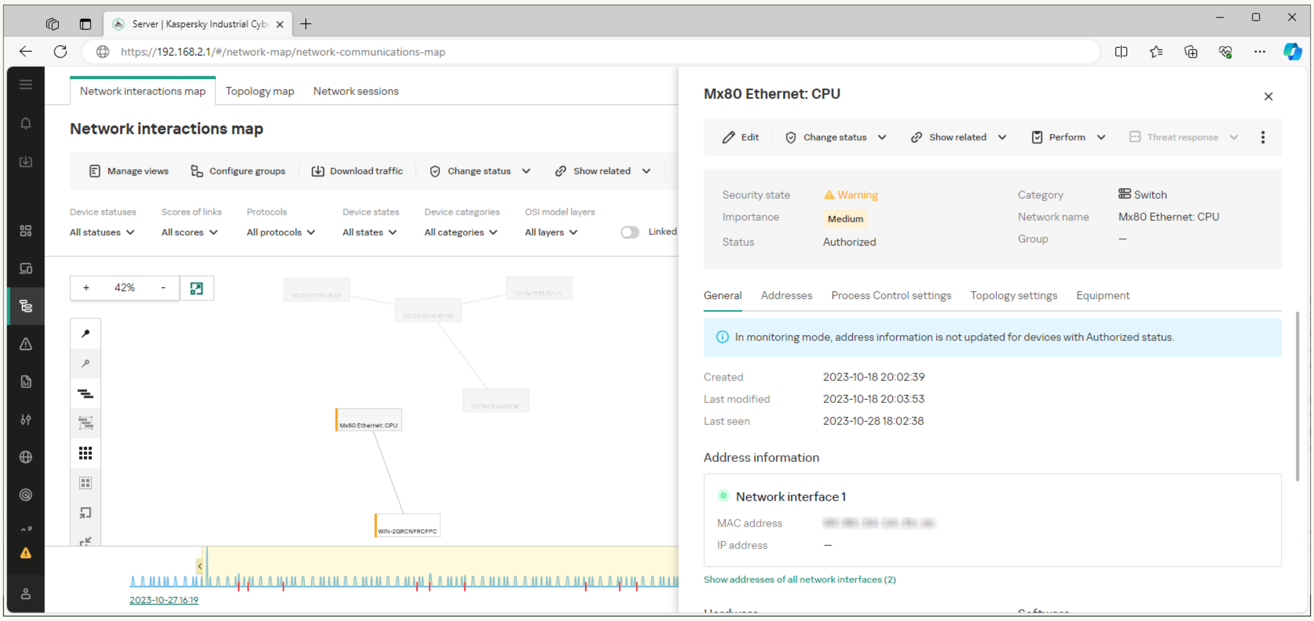
Assets section

The **Assets** section contains tabs with tables of devices and address spaces.

When asset is selected, the details area opens in the right part of the section. When an address space is selected, a block opens with information about its rules and subnets. When a device or subnet is selected, the details area opens in the right part of the section. The details area contains information about the selected elements and the tools for managing them.

- – opens the Network map section.

In the **Network map** section of the Application Server web interface (see the figure below), you can view information about the interactions and physical connections of devices.



Security state: ⚠ Warning
Importance: Medium
Status: Authorized
Category: Switch
Network name: Mx80 Ethernet: CPU
Group: –

In monitoring mode, address information is not updated for devices with Authorized status.

Created: 2023-10-18 20:02:39
Last modified: 2023-10-18 20:03:53
Last seen: 2023-10-28 18:02:38

Network interface 1
MAC address: [redacted]
IP address: –

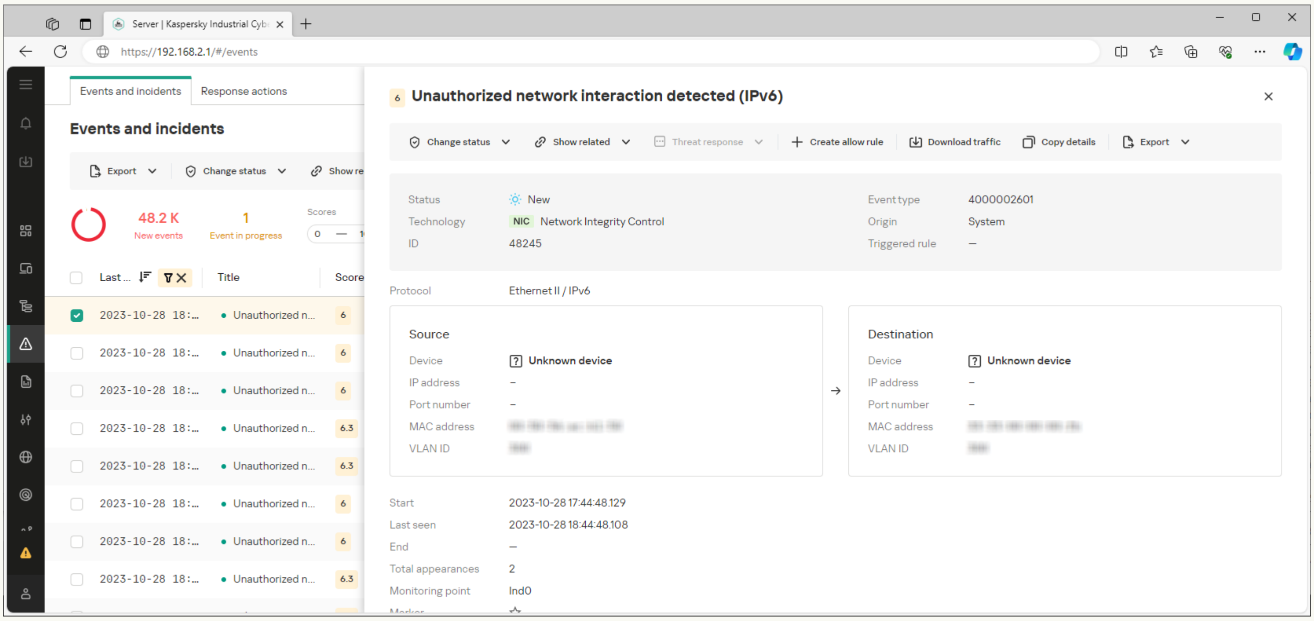
Network map section

The **Network map** section contains tabs with the network interactions map, topology map, and network sessions table. The tabs with the network interactions map and topology map contain the main toolbar in the upper part, an area for displaying objects on the network map, and additional toolbars for managing the position of objects. The lower part of the **Network interactions map** tab contains a time scale for filtering objects by time period.

When objects are selected, the details area opens in the right part of the section. The details area contains information about the selected objects and the tools for managing them.

- ⚠ – opens the Events section.

In the **Events** section of the Application Server web interface (see the figure below), you can view and process events and incidents registered by the application, and view the registered threat response actions.



Events and incidents

48.2 K New events

1 Event in progress

Scores 0 — 1

☐	Last ...	Title	Score
☑	2023-10-28 18:...	● Unauthorized n...	6
☐	2023-10-28 18:...	● Unauthorized n...	6
☐	2023-10-28 18:...	● Unauthorized n...	6
☐	2023-10-28 18:...	● Unauthorized n...	6.3
☐	2023-10-28 18:...	● Unauthorized n...	6.3
☐	2023-10-28 18:...	● Unauthorized n...	6
☐	2023-10-28 18:...	● Unauthorized n...	6
☐	2023-10-28 18:...	● Unauthorized n...	6.3

6 **Unauthorized network interaction detected (IPv6)**

Status	New	Event type	4000002601
Technology	NIC Network Integrity Control	Origin	System
ID	48245	Triggered rule	–

Protocol Ethernet II / IPv6

Source		→	Destination	
Device	Unknown device		Device	Unknown device
IP address	–		IP address	–
Port number	–		Port number	–
MAC address	[redacted]		MAC address	[redacted]
VLAN ID	[redacted]		VLAN ID	[redacted]

Start 2023-10-28 17:44:48.129

Last seen 2023-10-28 18:44:48.108

End –

Total appearances 2

Monitoring point Ind0

Marker ☆

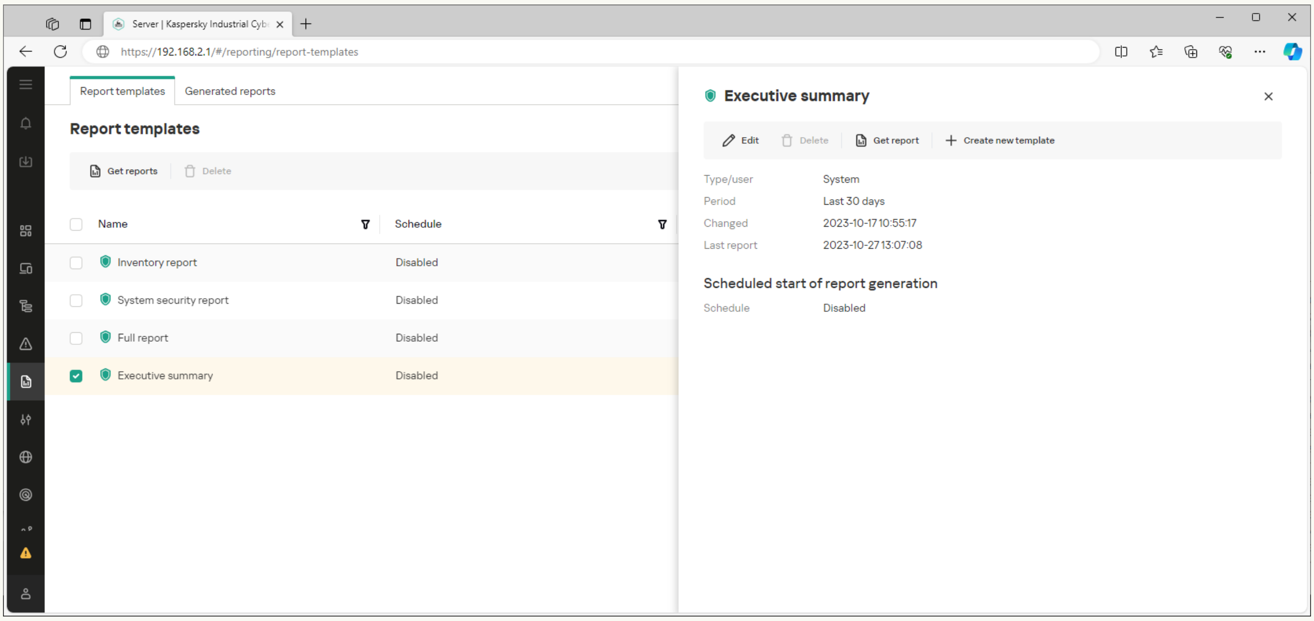
Events section

The **Events** section contains tabs with the events table and the response actions table.

When an event or action is selected, the details area opens in the right part of the section. The details area contains information about the selected objects and the tools for managing them.

- – opens the **Reports** section.

In the **Reports** section of the Application Server web interface (see the figure below), you can view information about report templates and change their settings. You can also view information about generated reports.



Report templates

Name	Schedule
Inventory report	Disabled
System security report	Disabled
Full report	Disabled
☑ Executive summary	Disabled

Executive summary

Type/user	System
Period	Last 30 days
Changed	2023-10-17 10:55:17
Last report	2023-10-27 13:07:08

Scheduled start of report generation

Schedule	Disabled

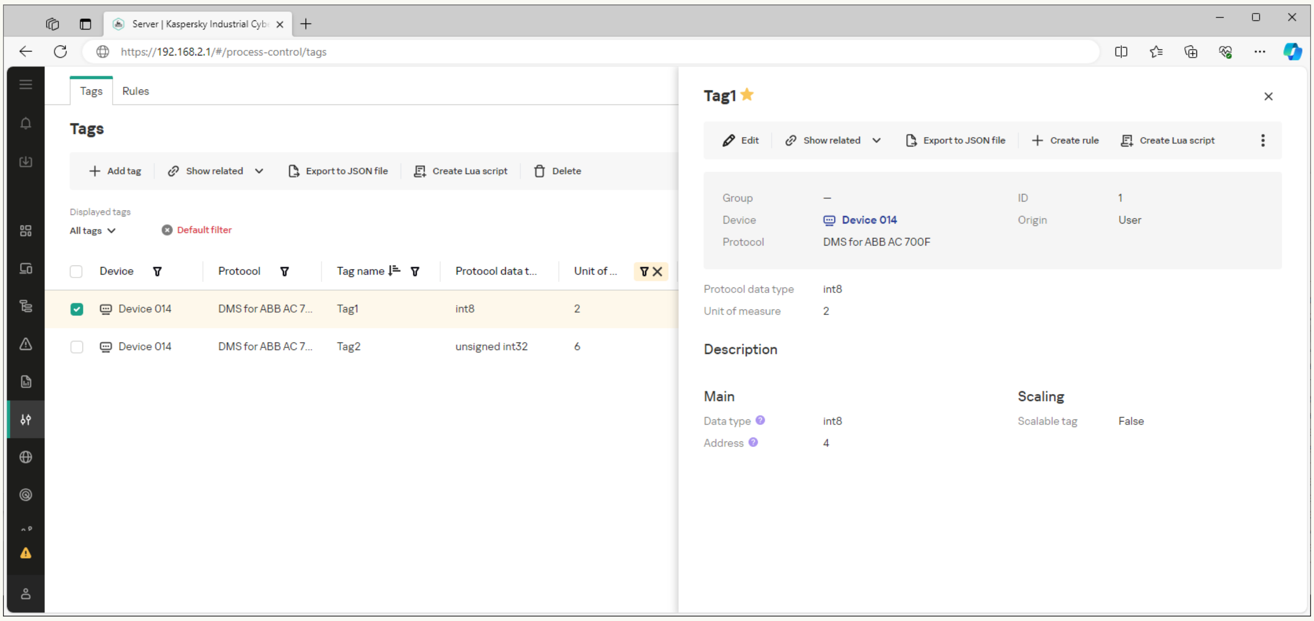
Reports section

The **Reports** section contains tabs with tables of report templates and generated reports.

When a report template or generated report is selected, the details area opens in the right part of the section. The details area contains information about the selected elements and the tools for managing them.

- – opens the **Process control** section.

In the **Process control** section of the Application Server web interface (see the figure below), you can view and edit tags and Process Control rules.



	Device	Protocol	Tag name	Protocol data t...	Unit of ...
☑	Device 014	DMS for ABB AC 7...	Tag1	int8	2
□	Device 014	DMS for ABB AC 7...	Tag2	unsigned int32	6

Group –
Device Device 014
Protocol DMS for ABB AC 700F
ID 1
Origin User

Protocol data type int8
Unit of measure 2

Description

Main
Data type int8
Address 4

Scaling
Scalable tag False

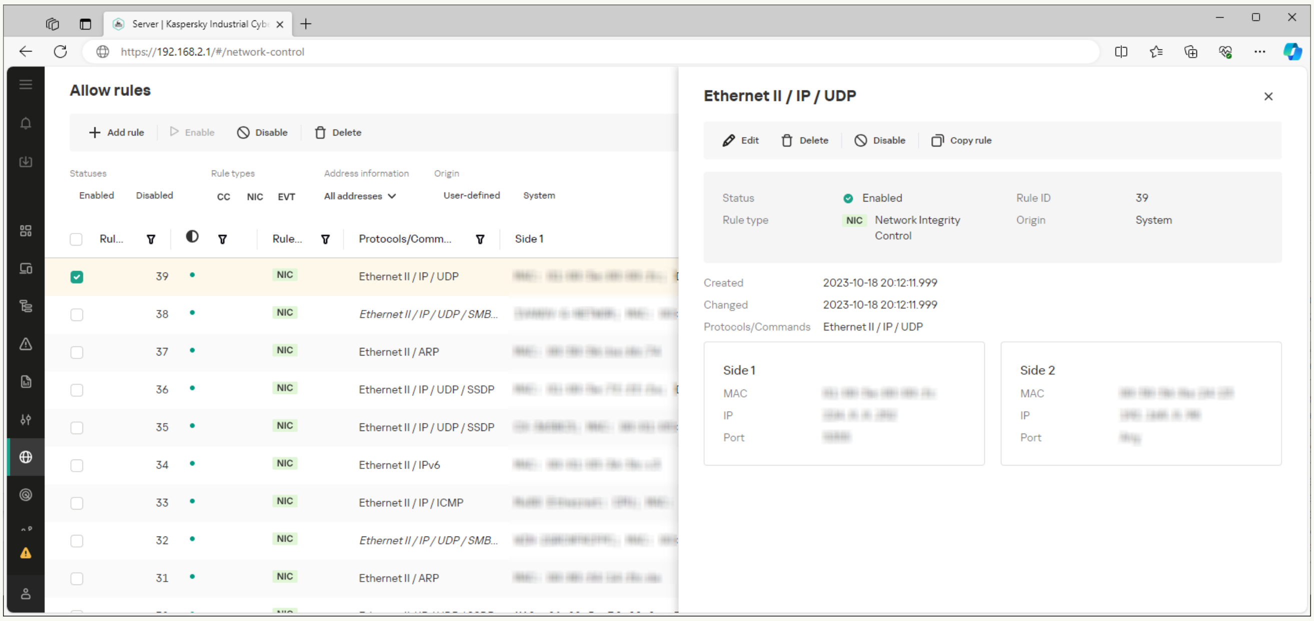
Process control section

The **Process control** section contains tabs with tables of tags and Process Control rules.

When a tag or rule is selected, the details area opens in the right part of the section. The details area contains information about the selected objects and the tools for managing them.

- – opens the Allow rules section.

In the **Allow rules** section of the Application Server web interface (see the figure below), you can view and edit allow rules for the application.



Allow rules

Statuses: Enabled, Disabled — Rule types: CC, NIC, EVT — Address information: All addresses — Origin: User-defined, System

	Rul...		Rule...	Protocols/Comm...	Side 1
☑	39	●	NIC	Ethernet II / IP / UDP	[redacted]
□	38	●	NIC	*Ethernet II / IP / UDP / SMB...*	[redacted]
□	37	●	NIC	Ethernet II / ARP	[redacted]
□	36	●	NIC	Ethernet II / IP / UDP / SSDP	[redacted]
□	35	●	NIC	Ethernet II / IP / UDP / SSDP	[redacted]
□	34	●	NIC	Ethernet II / IPv6	[redacted]
□	33	●	NIC	Ethernet II / IP / ICMP	[redacted]
□	32	●	NIC	*Ethernet II / IP / UDP / SMB...*	[redacted]
□	31	●	NIC	Ethernet II / ARP	[redacted]

Ethernet II / IP / UDP

Status	Enabled	Rule ID	39
Rule type	NIC Network Integrity Control	Origin	System

Created 2023-10-18 20:12:11.999
Changed 2023-10-18 20:12:11.999
Protocols/Commands Ethernet II / IP / UDP

Side 1		Side 2	
MAC	[redacted]	MAC	[redacted]
IP	[redacted]	IP	[redacted]
Port	[redacted]	Port	[redacted]

Server | Kaspersky Industrial Cyb
https://192.168.2.1/#/network-control
Add rule
Enable
Disable
Delete
Edit
Delete
Disable
Copy rule

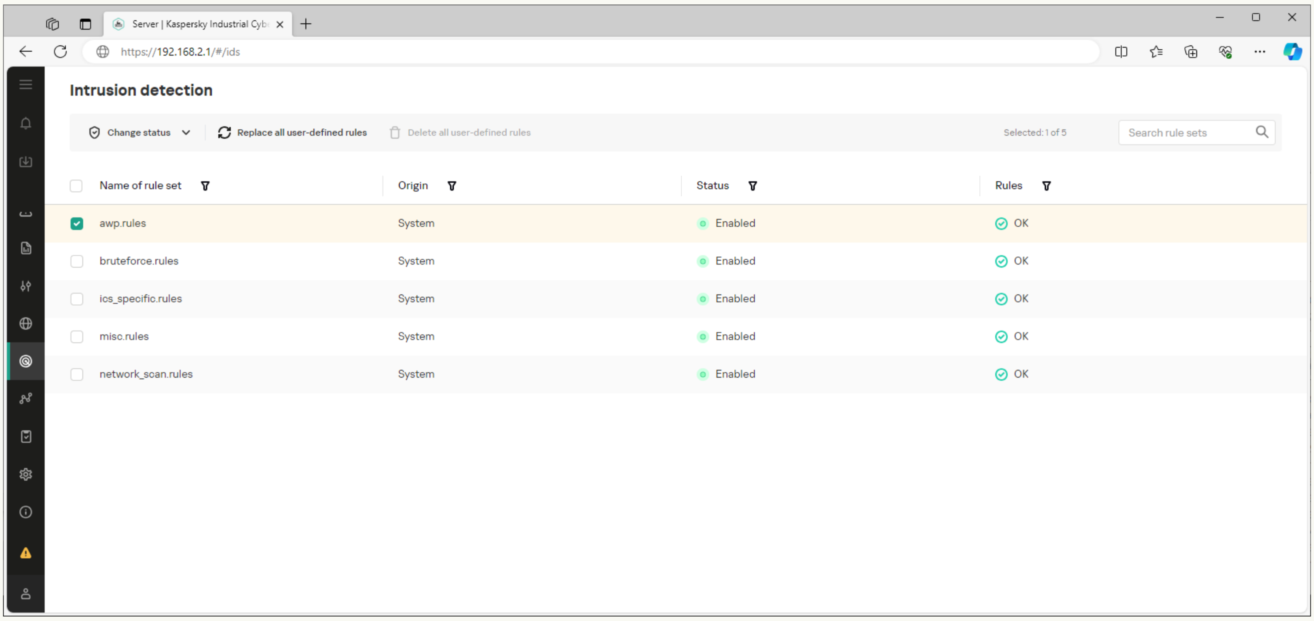
Allow rules section

The **Allow rules** section contains a table of allow rules for Interaction Control and for events.

When a rule is selected, the details area opens in the right part of the section. The details area contains information about the selected rule and the tools for managing it.

- ◎ – opens the **Intrusion detection** ? section.

In the **Intrusion detection** section of the Application Server web interface (see the figure below), you can manage sets of Intrusion Detection rules.



Intrusion detection

Selected: 1 of 5

	Name of rule set	Origin	Status	Rules
☑	awp.rules	System	Enabled	✓ OK
□	bruteforce.rules	System	Enabled	✓ OK
□	ics_specific.rules	System	Enabled	✓ OK
□	misc.rules	System	Enabled	✓ OK
□	network_scan.rules	System	Enabled	✓ OK

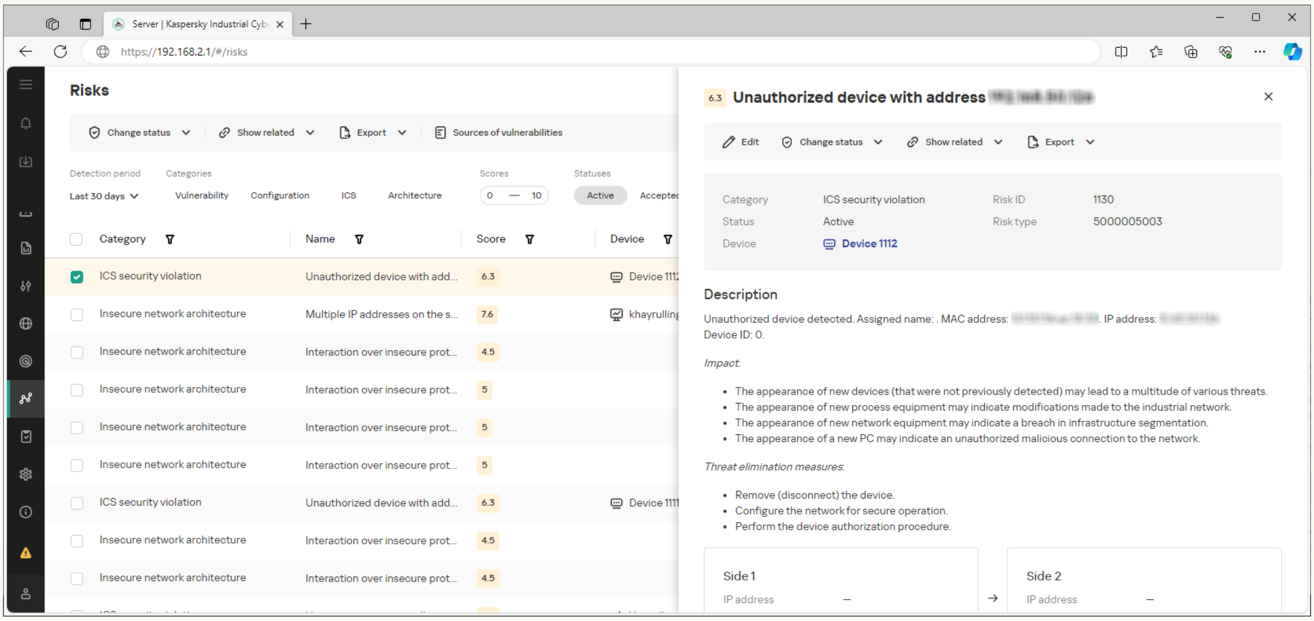
Server | Kaspersky Industrial Cyb
https://192.168.2.1/#/ids
Change status
Replace all user-defined rules
Delete all user-defined rules
Search rule sets

Intrusion detection section

The **Intrusion detection** section contains a toolbar and a table containing sets of rules.

- ⛗ – opens the **Risks** ? section.

In the **Risks** section of the Application Server web interface (see the figure below), you can view and resolve risks that could affect information system resources.



☐	Category	Name	Score	Device
☑	ICS security violation	Unauthorized device with add...	6.3	Device 1112
☐	Insecure network architecture	Multiple IP addresses on the s...	7.6	khayrulling
☐	Insecure network architecture	Interaction over insecure prot...	4.5	
☐	Insecure network architecture	Interaction over insecure prot...	5	
☐	Insecure network architecture	Interaction over insecure prot...	5	
☐	Insecure network architecture	Interaction over insecure prot...	5	
☐	ICS security violation	Unauthorized device with add...	6.3	Device 1111
☐	Insecure network architecture	Interaction over insecure prot...	4.5	
☐	Insecure network architecture	Interaction over insecure prot...	4.5	

6.3 **Unauthorized device with address** [redacted]

Category	ICS security violation	Risk ID	1130
Status	Active	Risk type	5000005003
Device	Device 1112		

Description

Unauthorized device detected. Assigned name: . MAC address: [redacted]. IP address: [redacted]. Device ID: 0.

Impact:

- The appearance of new devices (that were not previously detected) may lead to a multitude of various threats.
- The appearance of new process equipment may indicate modifications made to the industrial network.
- The appearance of new network equipment may indicate a breach in infrastructure segmentation.
- The appearance of a new PC may indicate an unauthorized malicious connection to the network.

Threat elimination measures:

- Remove (disconnect) the device.
- Configure the network for secure operation.
- Perform the device authorization procedure.

Side 1
IP address –

Side 2
IP address –

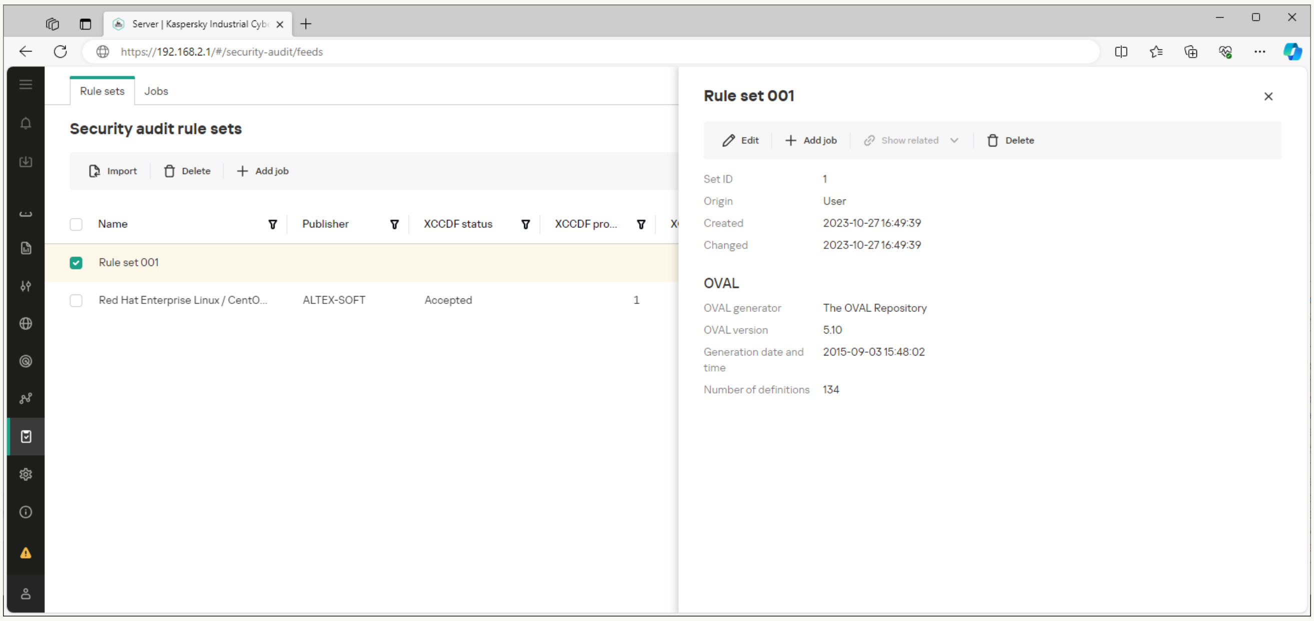
Risks section

The **Risks** section contains the risks table.

When a risk is selected, the details area opens in the right part of the section. The details area contains information about the selected risk and the tools for managing it.

- ▣ – opens the **Security audit** ? section.

In the **Security audit** section of the Application Server web interface (see the figure below), you can view and edit security audit jobs and sets of rules, and manage security audit jobs.


Server | Kaspersky Industrial Cyb
https://192.168.2.1/#/security-audit/feeds
Rule sets
Jobs
Import
Delete
Add job
Edit
Add job
Show related
Delete

Security audit rule sets

☐	Name	Publisher	XCCDF status	XCCDF pro...	X
☑	Rule set 001				
☐	Red Hat Enterprise Linux / CentO...	ALTEX-SOFT	Accepted	1	

Rule set 001

Set ID 1
Origin User
Created 2023-10-27 16:49:39
Changed 2023-10-27 16:49:39

OVAL

OVAL generator The OVAL Repository
OVAL version 5.10
Generation date and time 2015-09-03 15:48:02
Number of definitions 134

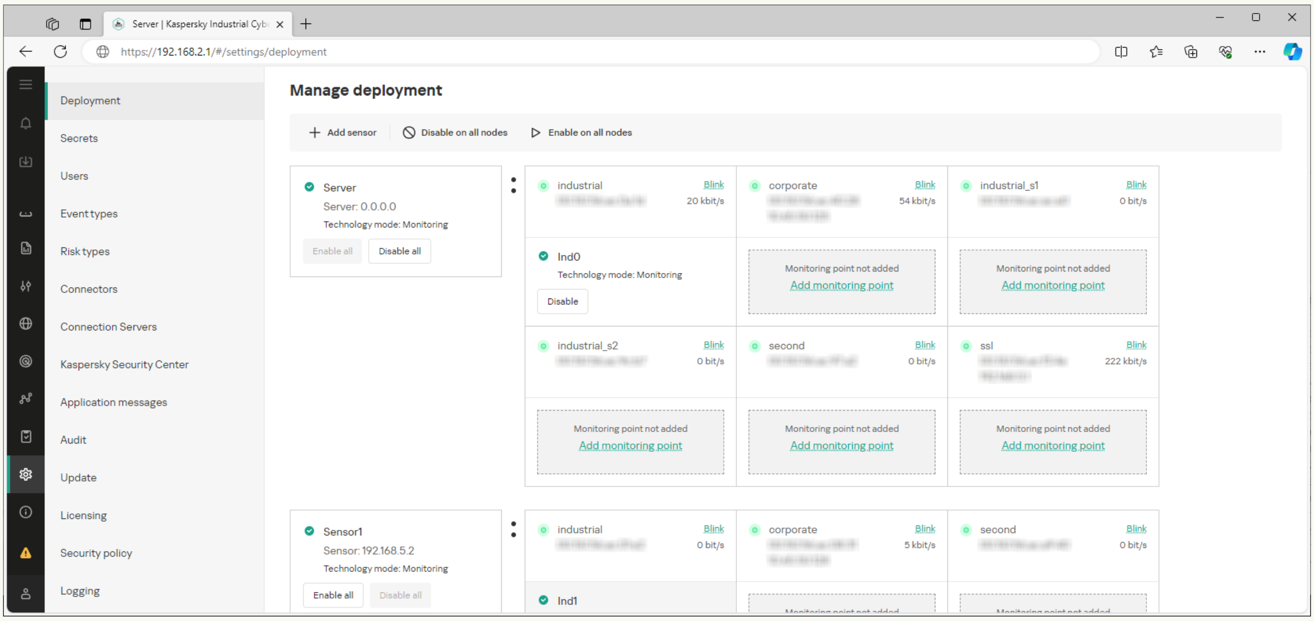
Security audit section

The **Security audit** section contains tabs with the security audit rule sets table and the security audit jobs table.

When a rule or rule set is selected, the details area opens in the right part of the section. The details area contains information about the selected objects and the tools for managing them.

- ⚙ – opens the **Settings** section.

In the **Settings** section of the Application Server web interface (see the figure below), you can view and edit application settings.



Settings section

When you select the **Settings** section, an additional menu appears on the web interface page. In this menu, you can go to the following subsections:

- **Deployment**.

  In this section, you can view information about nodes that have application components installed, and information about monitoring points on nodes. If an Administrator account is used to connect to the Server, you can also manage deployment settings in this section.

- **Secrets**.

  In this section, you can manage secrets containing account credentials for remote connections. The **Secrets** section is displayed if an Administrator account was used to connect to the Server.

- **Users**.

  In this section, you can manage application user accounts. The **Users** section is displayed if an Administrator account was used to connect to the Server.

- **Event types**.

  In this section, you can view and edit the settings of event types.

- **Connectors**.

  In this section, you can manage connectors for the application.

- **Connection Servers**.

  In this section, you can view and edit the settings of the web server on the computer hosting the Server (for example, to use a trusted certificate), REST API server and integration servers on nodes.

- **Kaspersky Security Center**.

  In this section, you can view and edit the settings for connecting to the Kaspersky Security Center Administration Server (if the capability for application interaction with Kaspersky Security Center has been added).

  - **Application messages**.

    In this section, you can view application messages.

  - **Audit**.

    In this section, you can view audit log entries and enable or disable the user activity audit. The **Audit** section is displayed if a user account with the Administrator role was used to connect to the Server.

  - **Update**.

    In this section, you can configure and run updates of application modules and databases.

  - **Licensing**.

    In this section, you can manage the license key for updating application modules and databases.

  - **Security policy**.

    In this section, you can manage the application security policy.

  - **Logging**.

    In this section, you can configure the logging levels for process logs.

- ⓘ – opens a section containing brief information about the application.

- ⚠ – displayed if some application functions are disabled or if learning mode is enabled for functions. When the menu is maximized, the **Not all protection services are running** notification is displayed. Clicking this icon or text opens a window containing information about disabled protection functions.

- **Connection Server** – displays the name of the Server to which the connection was established (the name defined during initial configuration of the application after installation).

- 👤 – opens and closes the user menu if the menu is collapsed. If the menu is expanded, nearby you will see the name of the current user and its role (in this case, you can use the button on the right to open and close the user menu). The user menu consists of the following sections:

  - **Language** – lets you select the language of the application web interface: English or Russian.

    > The selected localization language of the application web interface does not affect the localization language of the Kaspersky Industrial CyberSecurity for Networks Server. This component uses the localization language that was defined during installation or reinstallation of Kaspersky Industrial CyberSecurity for Networks. Therefore, the localization language of data provided by the Server may differ from the selected localization language of the web interface. For example, events and messages received from the Server (including some error messages) are displayed in the localization language of the Server.

  - **Theme** – lets you select the color design theme for the web interface page:

    - **Light** – items are displayed on a white background.

    - **Dark** – items are displayed on a dark background.

  - **User account** – groups menu items for performing actions with the account of the current user:

    - **Change password** – opens the window for changing the password of the current user.

    - **Log out** – ends the Server connection session and opens the page for entering the account credentials to connect.

- **Additional information** – contains the **Help** option for proceeding to the Online Help page of Kaspersky Industrial CyberSecurity for Networks.

Kaspersky Industrial CyberSecurity for Networks sensor web interface

When you connect to a Kaspersky Industrial CyberSecurity for Networks sensor through the web interface, the sensor web interface page opens in your browser. The contents of the web interface page depend on the state of the connection between the sensor and the Application Server.

Depending on the state of the connection between the sensor and the Application Server, the web interface page may contain the following management elements or data:

- Before connecting the sensor to the Server – management elements for selecting a communication data package and/or data for automatically connecting the sensor over the network.

- After connecting the sensor to the Server – data on the Server and sensor (including the capability to proceed to the Server web interface page) and the connection state.

Licensing the application

This section contains information about licensing Kaspersky Industrial CyberSecurity for Networks.

About the End User License Agreement

The *End User License Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the application.

Carefully read and accept the terms of the End User License Agreement before you start using the application.

You can view the terms of the End User License Agreement in the following ways:

- During initial configuration of the application.
- By opening the license_en.txt, that is a part of application distribution kit (the copy of this document is also saved in the application installation folder).

Read and accept the terms of the End User License Agreement during initial configuration of the application. If you do not accept the terms of the End User License Agreement, you must cancel the initial configuration of the application and must not use the application.

About the Privacy Policy

The *Privacy Policy* is a document that informs you about how your data is processed.

Carefully read and accept the terms of the Privacy Policy before you start using the application.

You can view the terms of the Privacy Policy as follows:

- During initial configuration of the application.
- By opening the privacy_policy_en.txt, that is a part of application distribution kit (the copy of this document is also saved in the application installation folder).

Please read and accept the terms of the Privacy Policy during initial configuration of the application. If you do not accept the terms of the Privacy Policy, you must cancel the initial configuration of the application and must not use the application.

About the license

The *license* entitles you to use the application under the End User License Agreement. You can use the application functionality if you purchase a license certificate.

The following types of licenses are provided for the current application version:

- Base—to use the application functions, except for Updating databases and application modules, Active polling of devices, and Security audit.

  This type of license has no time limit and does not require you to add a license key to the application.

- Upd&Sup – for use of update functionality for databases and application modules on the Server and sensors.

  This type of license has a time limit. To enable the update functionality, add the license key with a valid Upd&Sup license to the application (you can also use the license key for the previous application versions with a valid Limited Updates license). When this type of license expires, the application continues to work, but update functionality becomes unavailable. In this case, to continue the use of the update function, add a new license key.

- Security Audit is for using the Security audit functionality and the Active device polling functionality.

  This type of license has a time limit. To enable the Security audit and the Active polling of devices functionality, add the license key with a valid Security Audit license to the application (you can also use the license key for the previous application versions with a valid Active Polling license). After the license of this type expires, the application continues to work, but the Security audit and the Active polling of devices functions are no longer available. In this case, to continue using the specified functions, add a new license key with a valid license of this type.

Using a license key, you can activate either only the function for the Upd&Sup license type or both the function for the Upd&Sup license type and the function for the Security Audit license type. Only one license key can be added to the application. You can view information about the added license key when connected to the Server through the web interface.

Kaspersky software updates including antivirus signatures and the codebase will be unavailable in the United States starting at 12:00 AM Eastern Daylight Time (EDT) on September 10, 2024 in accordance with restrictions.

Technical support services are provided if you have an active Technical Support Agreement. To receive technical support services, you must appoint contact persons who are authorized to open requests for technical support services.

About the license certificate

The *license certificate* is a document that confirms your right to use the application. This document is provided to you when you purchase a license.

A license certificate for Kaspersky Industrial CyberSecurity for Networks contains the following information:

- License key or order number
- Information about the user who is granted the license
- Information about the application and the component covered by the license
- Restriction on the number of licensing units (for example, the number of sensors)
- Start date of the license term
- License expiration date or license term
- License type

About the license key used for activating application functionality

A *license key* (hereinafter also referred to as simply "key") is a sequence of bits with which you can activate and subsequently use the corresponding application functionality in accordance with the terms of the End User License Agreement. Depending on the purpose of the particular license key, you can use it to activate the functionality for updating application modules and databases or simultaneously activate active device polling functionality together with the functionality for updating application modules and databases. The license key is generated by Kaspersky experts.

You can add a license key to the application by using a *license key file*. After you add a license key to the application, the license key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky can block a license key over violations of the End User License Agreement. If the license key is blocked, you have to add a different license key to use the corresponding application functionality.

About the license key file

A *license key file* is a file with the KEY extension that you receive from Kaspersky. The license key file is used to add a license key that activates the corresponding application functionality.

You receive a license key file after you purchase Kaspersky Industrial CyberSecurity for Networks. The method used to receive a license key file is determined by the Kaspersky distributor from whom you purchased the application (for example, the license key file may be sent to the email address you specify).

You can also add a license key from a license key file that was received when purchasing a previous version of Kaspersky Industrial CyberSecurity for Networks. A license key can be added to the application before its expiration date.

You do not need to connect to Kaspersky activation servers to activate application functionality with a license key file.

Adding a license key when connected to the Server through the web interface

You can add a license key to Kaspersky Industrial CyberSecurity for Networks when connected to the Server through the web interface or by using the functionality for automatic distribution of license keys to Kaspersky Security Center.

Only users with the Administrator role can add a license key.

To add a license key:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Licensing**.
3. Click the **Add license key** button. This button is absent if a license key has already been added to the application.

   This opens the standard browser window for selecting a license key file.

4. Specify the path to the license key file with the KEY extension.

5. Click the button for opening the file.

   The license key from the selected key file will be loaded into the application.

Viewing information about an added license key

You can view information about the added license key when connected to the Server through the web interface. Information about the license key is displayed under **Settings** → **Licensing**. The list of notifications about application operating issues may also display warnings about the license key status.

To view information about the license key:

Select **Settings** → **Licensing**.

The following information is displayed for an added license key:

- **Key** – unique alphanumeric sequence.
- **Description** – information about available functionality.
- **Activation date** – date when the license key was first added to the application.
- **Validity term** – expiration date of the license key.
- **Expires** – number of days remaining until expiration.
- Information about the key status or warning about a problem.

Removing a license key

When connected to the Server through the web interface, you can remove an added license key from the application (for example, if you need to replace the current license key with a different key). After the license key is removed, the corresponding functionality is no longer available in the application. This unavailable functionality will be re-activated the next time you add a license key.

Only users with the Administrator role can delete a license key.

To remove an added license key:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Licensing**.

3. Click the **Delete** button.

   A window with a confirmation prompt opens.

4. Confirm deletion of the license key.

The license key will be removed from the application.

Data provision

The terms and conditions of the End User License Agreement describe the data processed automatically to provide the proper application operation. The right holder processes the provided data in accordance with the Privacy Policy describing, in particular, data protection measures, processing locations, and data subjects' rights. In certain countries, some of the provided data can be categorized as personal data according to the legislation.

The application does not send users' personal data to Kaspersky. Users' personal data is processed on the computers on which the application components are installed.

The application processes and saves the following data related to users' personal data:

- Names of user accounts that were created in the application (application users).
- IP addresses or names of computers with application components installed.
- IP addresses, MAC addresses, and other device information received by the application.
- Data on address spaces and subnets.
- Data on industrial process settings in Process Control rules.
- IP address or name of the computer hosting Kaspersky Security Center.
- IP addresses or names of computers that connect to the application through connectors.
- Email addresses of recipients indicated in email connectors and in report templates.
- Data in generated application reports.
- Data in industrial network traffic transmitted between devices and containing users' personal data (this data is processed by the application together with other data when analyzing industrial network traffic).
- Data on detected risks that could affect industrial system resources.
- Data on possibly infected objects or potential threats received from EPP applications and containing IP addresses, web addresses, and email addresses.
- Data on user accounts received from EPP applications.
- Application data received from EPP applications.

The listed data is processed for the purpose of analyzing process violations and for detecting network traffic anomalies and other threats that may be signs of attacks.

The application saves the received data in logs.

If the application administrator has configured forwarding of application data to recipient systems, the received data is processed and stored in the recipient system in accordance with its functionality and purpose.

If the application centralized installation script was used to create files for the purpose of providing information to Kaspersky Technical Support, the following data is saved in these files:

- Contents of folders used for storing application data:
  - Files of process logs for application components, the DBMS, and the Intrusion Detection system.

    - Files of working data of the Server and sensors.
    - Installation settings file created by the application centralized installation script.
    - Application message log and audit log.
- Security policy applied on the Server.
- Information about the current status of services that support the operation of application components:
    - kics4net
    - kics4net-apm
    - kics4net-asset-inventory
    - kics4net-blob-storage
    - kics4net-connectors
    - kics4net-connectors-launcher
    - kics4net-email-gateway
    - kics4net-epp-proxy
    - kics4net-fts
    - kics4net-nats-server
    - kics4net-oval-facade
    - kics4net-postgresql
    - kics4net-report-builder
    - kics4net-report-data-source
    - kics4net-report-renderer
    - kics4net-report-templates-catalog
    - kics4net-report-templates-catalog-view
    - kics4net-responses-manager
    - kics4net-risk-oval-detector
    - kics4net-scan-oval-manager
    - kics4net-scap-manager
    - kics4net-scap-manager-view
    - kics4net-scheduler

    - kics4net-secrets
    - kics4net-task-manager
    - kics4net-task-manager-view
    - kics4net-vault
    - kics4net-webserver
    - kics4net-websensor
    - klnagent
- Information about the version and distribution package of the operating system on computers that have application components installed (the `uname -a` command is used for receiving information).
- Information about the network interfaces on computers that have application components installed (the `ifconfig` command is used for receiving information).
- Entries saved by the auditd service in the file /var/log/audit/audit.log.
- Settings, status, and operating mode of the firewall in the operating system.
- If the corresponding settings are defined, the following files and data are also saved when running the application centralized installation script:
    - Traffic dump files.
    - Data on the Intrusion Detection system configuration.
    - Data on the certificates used in Kaspersky Industrial CyberSecurity for Networks (except certificates that were published by trusted certificate authorities).

The application does not monitor access to the installation settings file created by the application centralized installation script. However, the application does track startups of application components and other connections to the Server that involve verification of user credentials.

When receiving updates from Kaspersky servers, the application transmits data necessary for automatic selection of relevant updates. Transmitted data does not contain any personal data of users. The application transmits the following data:

- Version of Kaspersky Industrial CyberSecurity for Networks.
- Localization language code of components of Kaspersky Industrial CyberSecurity for Networks.
- IDs of updated elements.
- Kaspersky Industrial CyberSecurity for Networks installation ID.
- ID of the type, version and bit rate of the operating system.

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.

Folders for storing application data

Deleting or modifying any file in these folders can affect the operation of the application.

On the Kaspersky Industrial CyberSecurity for Networks Server, the application uses the following folders and subfolders for storing data:

- Component and service installation folders:
  - /opt/kaspersky/kics4net/ – for the Server.
  - /opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /opt/kaspersky/kics4net-asset-inventory/ – for the service that processes the results of scanning device attributes using OVAL® rules.
  - /opt/kaspersky/kics4net-blob-storage/ – for the service that stores arrays of binary data. (Binary Large Object, BLOB).
  - /opt/kaspersky/kics4net-connectors/ – for system connectors.
  - /opt/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
  - /opt/kaspersky/kics4net-email-gateway/ – for the service of sending email notifications.
  - /opt/kaspersky/kics4net-epp-proxy/ – for the Kaspersky Endpoint Agent integration service.
  - /opt/kaspersky/kics4net-fts/ – for the full-text search system.
  - /opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /opt/kaspersky/kics4net-postgresql/ – for the DBMS.
  - /opt/kaspersky/kics4net-report-builder/ – for the service of generating reports.
  - /opt/kaspersky/kics4net-report-data-source/ – for the service of providing data for reports.
  - /opt/kaspersky/kics4net-report-renderer/ – for the service of visual representation of data blocks in reports.
  - /opt/kaspersky/kics4net-report-templates-catalog/ – for the service of managing report templates.
  - /opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service of providing data on report templates.
  - /opt/kaspersky/kics4net-task-manager/ – for the response task management service.

  - /opt/kaspersky/kics4net-risk-oval-detector/ – for the service for processing the results of the device scan for risks using the OVAL rules.
  - /opt/kaspersky/kics4net-scan-oval-manager/ – for the service for managing the device scan using OVAL rules.
  - /opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.
  - /opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
  - /opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.
  - /opt/kaspersky/kics4net-secrets/ – for the secrets repository facade.
  - /opt/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
  - /opt/kaspersky/kics4net-task-manager/ – for the task management service.
  - /opt/kaspersky/kics4net-task-manager-view/ – for the service of providing data on tasks.
  - /opt/kaspersky/kics4net-vault/ – for the service for storing the secrets in the repository.
  - /opt/kaspersky/kics4net-webserver/ – for the web server.
  - /opt/kaspersky/klnagent64/ – for Network Agent.
- Folders for storing certificates and operational data:
  - /opt/kaspersky/kics4net/share/ids/ – for the Intrusion Detection system.
  - /var/opt/kaspersky/kics4net/ – for the Server.
  - /var/opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/opt/kaspersky/kics4net-asset-inventory/ – for the service of processing the results of the device attribute scan using the OVAL rules.
  - /var/opt/kaspersky/kics4net-blob-storage/ – for the BLOB service.
  - /var/opt/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
  - /var/opt/kaspersky/kics4net-email-gateway/ – for the service of sending email notifications.
  - /var/opt/kaspersky/kics4net-epp-proxy/ – for the integration service.
  - /var/opt/kaspersky/kics4net-fts/ – for the full-text search system.
  - /var/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /var/opt/kaspersky/kics4net-oval-facade/ – for the service for scanning remote devices using OVAL rules.
  - /var/opt/kaspersky/kics4net-postgresql/ – for the DBMS.

  - /var/opt/kaspersky/kics4net-report-builder/ – for the service of generating reports.
  - /var/opt/kaspersky/kics4net-report-data-source/ – for the service of providing data for reports.
  - /var/opt/kaspersky/kics4net-report-renderer/ – for the service of presenting data blocks in reports.
  - /var/opt/kaspersky/kics4net-report-templates-catalog/ – for the service of managing report templates.
  - /var/opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service of providing data on report templates.
  - /var/opt/kaspersky/kics4net-responses-manager/ – for the response task management service.
  - /var/opt/kaspersky/kics4net-risk-oval-detector/ – for the service of processing the results of the device scan for risks using the OVAL rules.
  - /var/opt/kaspersky/kics4net-scan-oval-manager/ – for the service for managing the device scan using OVAL rules.
  - /var/opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.
  - /var/opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
  - /var/opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.
  - /var/opt/kaspersky/kics4net-task-manager/ – for the task management service.
  - /var/opt/kaspersky/kics4net-task-manager-view/ – for the service of providing data on tasks.
  - /var/opt/kaspersky/kics4net-vault/ – for the service for storing the secrets in the repository.
  - /var/opt/kaspersky/kics4net-webserver/ – for the web server.
  - /var/opt/kaspersky/klnagent/ – for Network Agent.
- Folders for storing process logs:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were centrally installed from this computer).
  - /var/log/kaspersky/kics4net/ – for the Server.
  - /var/log/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/log/kaspersky/kics4net-asset-inventory/ – for the service of processing the results of the device attribute scan using the OVAL rules.
  - /var/log/kaspersky/kics4net-blob-storage/ – for the BLOB service.
  - /var/log/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/log/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
  - /var/log/kaspersky/kics4net-email-gateway/ – for the service of sending email notifications.

  - /var/log/kaspersky/kics4net-epp-proxy/ – for the integration service.
  - /var/log/kaspersky/kics4net-fts/ – for the full-text search system.
  - /var/log/kaspersky/kics4net-nats-server/ – for the message broker.
  - /var/log/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /var/log/kaspersky/kics4net-postgresql/ – for the DBMS.
  - /var/log/kaspersky/kics4net-report-builder/ – for the service of generating reports.
  - /var/log/kaspersky/kics4net-report-data-source/ – for the service of providing data for reports.
  - /var/log/kaspersky/kics4net-report-renderer/ – for the service of presenting data blocks in reports.
  - /var/log/kaspersky/kics4net-report-templates-catalog/ – for the service of managing report templates.
  - /var/log/kaspersky/kics4net-report-templates-catalog-view/ – for the service of providing data on report templates.
  - /var/log/kaspersky/kics4net-responses-manager/ – for the response task management service.
  - /var/log/kaspersky/kics4net-risk-oval-detector/ – for the service of processing the results of the device scan for risks using the OVAL rules.
  - /var/log/kaspersky/kics4net-scan-oval-manager/ – for the service for managing the device scan using OVAL rules.
  - /var/log/kaspersky/kics4net-scap-manager/ – for the security audit management service.
  - /var/log/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
  - /var/log/kaspersky/kics4net-scheduler/ – for the task scheduling service.
  - /var/log/kaspersky/kics4net-secrets/ – for the secrets repository facade.
  - /var/log/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
  - /var/log/kaspersky/kics4net-task-manager/ – for the task management service.
  - /var/log/kaspersky/kics4net-task-manager-view/ – for the service of providing data on tasks.
  - /var/log/kaspersky/kics4net-vault/ – for the service for storing the secrets in the repository.
  - /var/log/kaspersky/kics4net-webserver/ – for the web server (the web server also saves process data in the system log of the operating system).
  - /var/log/kaspersky/klnagent64/ – for Network Agent.
- Folders for storing configuration files:
  - /etc/opt/kaspersky/kics4net/ – for the Server.

- /etc/opt/kaspersky/kics4net-asset-inventory/ – for the service of processing the results of the device attribute scan using the OVAL rules.

- /etc/opt/kaspersky/kics4net-blob-storage/ – for the BLOB service.

- /etc/opt/kaspersky/kics4net-email-gateway/ – for the service of sending email notifications.

- /etc/opt/kaspersky/kics4net-epp-proxy/ – for the integration service.

- /etc/opt/kaspersky/kics4net-fts/ – for the full-text search system.

- /etc/opt/kaspersky/kics4net-nats-server/ – for the message broker.

- /etc/opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.

- /etc/opt/kaspersky/kics4net-report-builder/ – for the service of generating reports.

- /etc/opt/kaspersky/kics4net-report-data-source/ – for the service of providing data for reports.

- /etc/opt/kaspersky/kics4net-report-renderer/ – for the service of presenting data blocks in reports.

- /etc/opt/kaspersky/kics4net-report-templates-catalog/ – for the service of managing report templates.

- /etc/opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service of providing data on report templates.

- /etc/opt/kaspersky/kics4net-responses-manager/ – for the response task management service.

- /etc/opt/kaspersky/kics4net-risk-oval-detector/ – for the service of processing the results of the device scan for risks using the OVAL rules.

- /etc/opt/kaspersky/kics4net-scan-oval-manager/ – for the service for managing the device scan using OVAL rules.

- /etc/opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.

- /etc/opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.

- /etc/opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.

- /etc/opt/kaspersky/kics4net-secrets/ – for the secrets repository facade.

- /etc/opt/kaspersky/kics4net-task-manager/ – for the task management service.

- /etc/opt/kaspersky/kics4net-task-manager-view/ – for the service of providing data on tasks.

- /etc/opt/kaspersky/kics4net-vault/ – for the service for storing the secrets in the repository.

- /etc/opt/kaspersky/kics4net-webserver/ – for the web server.

- /etc/opt/kaspersky/klnagent/ – for Network Agent.

- /usr/lib/systemd/system/ – for storing configuration files for Kaspersky Industrial CyberSecurity for Networks services (for example, kics4net.service).

    - /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file created during centralized installation of the application.
    - /var/run/ – for storing variables of data on system health after loading in the folder itself (for example, the klnagent.pid file), or in subfolders (for example, the /kics4net/ subfolder).

On the Kaspersky Industrial CyberSecurity for Networks sensor, the application uses the following folders and subfolders for storing data:

- Component and service installation folders:
    - /opt/kaspersky/kics4net/ – for the sensor.
    - /opt/kaspersky/kics4net-apm/ – for the active polling connector.
    - /opt/kaspersky/kics4net-connectors/ – for system connectors.
    - /opt/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
    - /opt/kaspersky/kics4net-epp-proxy/ – for the integration service.
    - /opt/kaspersky/kics4net-nats-server/ – for the message broker.
    - /opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
    - /opt/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
    - /opt/kaspersky/kics4net-websensor/ – for the web server.
- Folders for storing certificates and operational data:
    - /opt/kaspersky/kics4net/share/ids/ – for the Intrusion Detection system.
    - /var/opt/kaspersky/kics4net/ – for the sensor.
    - /var/opt/kaspersky/kics4net-apm/ – for the active polling connector.
    - /var/opt/kaspersky/kics4net-connectors/ – for system connectors.
    - /var/opt/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
    - /var/opt/kaspersky/kics4net-epp-proxy/ – for the integration service.
    - /var/opt/kaspersky/kics4net-nats-server/ – for the message broker.
    - /var/opt/kaspersky/kics4net-oval-facade/ – for the device scan service using OVAL rules without the Network Agent.
    - /var/opt/kaspersky/kics4net-websensor/ – for the web server.
- Folders for storing process logs:

  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were centrally installed from this computer).
  - /var/log/kaspersky/kics4net/ – for the sensor.
  - /var/log/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/log/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/log/kaspersky/kics4net-connectors-launcher/ – for the service of registering and launching manageable connectors.
  - /var/log/kaspersky/kics4net-epp-proxy/ – for the integration service.
  - /var/log/kaspersky/kics4net-nats-server/ – for the message broker.
  - /var/log/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /var/log/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
  - /var/log/kaspersky/kics4net-websensor/ – for the web server (the web server also saves process data in the system log of the operating system).
- Folders for storing configuration files:
  - /etc/opt/kaspersky/kics4net/ – for the sensor.
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – for the integration service.
  - /etc/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /etc/opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /etc/opt/kaspersky/kics4net-websensor/ – for the web server.
  - /etc/opt/kaspersky/klnagent/ – for Network Agent.
  - /usr/lib/systemd/system/ – for storing configuration files for Kaspersky Industrial CyberSecurity for Networks services (for example, kics4net.service).
  - /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file created during centralized installation of the application.
  - /var/run/ – for storing variables of data on system health after loading in the folder itself or in subfolders.

Root privileges in the operating system are required for modifying the application files.

About logs

Kaspersky Industrial CyberSecurity for Networks saves data on its operation in logs. Depending on the type of log, the application saves data in the Server database or in files in local folders on the node of the Server or sensor.

Logs saved in the Server database

The application saves the following logs in the Server database:

- Log of events and incidents
- Audit log
- Application message log

You can view the contents of the listed logs when connected to the Server through the web interface.

If necessary, you can also configure data transfer from these logs to recipient systems through connectors.

Logs saved in files

Information about application processes is saved as files in local folders. Process log files may contain the following information:

- Data on the starting and stopping of Kaspersky Industrial CyberSecurity for Networks processes.
- Diagnostic messages that may be required when contacting Technical Support.
- Error messages.

Information about processes is stored according to the defined logging levels for processes.

You can use a text editor to view files containing process logs. Root privileges in the operating system are required for providing access to logs.

Files containing process logs are stored in non-encrypted form. You are advised to ensure protection against unauthorized access to information.

Administration of Kaspersky Industrial CyberSecurity for Networks

This section contains information about the actions performed for administration of Kaspersky Industrial CyberSecurity for Networks.

Deploying nodes

To deploy nodes with the installed application components, you can add or remove sensors, configure the settings for storing application data on nodes, and manage the protection functions.

If you use the Server without external sensors, you do not need to add sensors after installing the application. In this case, the deployment settings must be configured only for the Server node. To install the Server and external sensors, you can add sensors when connecting to the Server using the web interface. The application uses only the sensors that are added to the application and connected.

By default, the settings for storing the application data on the Server and sensors are set to ensure long-term storage and optimal use of free disk space. If necessary, you can change the data storage settings on any node taking into account the specifics of your system (for example, if the computer hardware does not fully meet the requirements).

The application monitors the operation of the available monitoring points and of the provided technologies in order to promptly notify the user about inactive protection functions of the application. If any monitoring points or technologies are disabled, the application displays a message about the disabled protection functions. This message is also displayed for technologies operating in the learning mode (this mode is available for some technologies). It is recommended to disable monitoring points and technologies, as well as to use the technology learning mode for a limited time. For example, you can disable a monitoring point for the period of maintenance and commissioning in the corresponding segment of the industrial network.

You can view information about the nodes and manage the deployment settings in the **Settings** → **Deployment** section of the Kaspersky Industrial CyberSecurity for Networks web interface. Only the users with the Administrator role can manage deployment settings.

Adding and deleting sensors

After installation and initial configuration of the Kaspersky Industrial CyberSecurity for Networks Server, you can add sensors to the application. Sensors are added on the Server web interface page.

To add a sensor on a computer, the corresponding packages must be installed from the application distribution kit. You can use the application components centralized installation script or local installation script to install these packages.

You can remove a sensor from the application. When a sensor is removed, the registration data of this sensor is deleted from the Application Server, which will make it impossible to connect the sensor to this Server.

However, the sensor component files will remain on this node after the sensor is removed. You can later add this node as a sensor again without having to install the corresponding packages. You can add the sensor to the current Server or to any other Kaspersky Industrial CyberSecurity for Networks Server that you can connect to.

Adding and connecting a sensor using the sensor web interface

When adding a sensor, a configuration package containing a certificate and configuration data for the sensor is generated on the Server. The added sensor is connected by using the sensor web interface. The sensor web interface lets you download the configuration package and connect the sensor using the following methods:

- Use a communication data package. When using this method, the configuration package is saved a file with password-protected certificate. This file is known as the *communication data package*. The communication data package must be securely delivered to a computer that can access the sensor computer over the network, and must then be downloaded on the sensor web interface page. After the communication data package is downloaded, the sensor is automatically connected to the Server on which this file was created.

  Using a communication data package to add and connect a sensor ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Click the **Add sensor** button.

   The details area appears in the right part of the web interface window.
4. On the **Using a communication data package** tab:
   a. Enter the sensor name that will represent the sensor within Kaspersky Industrial CyberSecurity for Networks.

      The sensor name must be unique (not match the names of other sensors or the Server) and must contain no more than 100 characters. You can use letters of the English alphabet, numerals, a space, and the following special characters: `_` and `-` (for example, `Sensor_1`). The sensor name must begin and end with any permitted character except a space.

   b. Enter the Server IP address that the sensor will use to connect to the Server.

   c. Enter the IP address used by the web server on the sensor computer.

   d. Enter password for protecting the certificate in the communication data package.

      The password must meet the following requirements:

      - Must contain between 8 and 256 ASCII characters.
      - Must contain one or more uppercase letters of the English alphabet.
      - Must contain one or more lowercase letters of the Latin alphabet.
      - Must contain one or more numerals.
      - Must contain no more than three consecutive repeated characters.
5. Click the **Create communication data package** button.

   Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.
6. Connect to the sensor through the web interface.
7. On the sensor web interface page, click the **Select file** button.

   This opens the standard browser window for selecting a file.
8. Specify the path to the communication data package.
9. Click the button for opening the file.
10. After downloading the contents of the file, enter the password for accessing the sensor certificate in the communication data package.

The sensor will connect to the Server, then information about the connection will be displayed on the Server and sensor web interface pages.

- Automatically over the network. This method lets you forward a configuration package over the network to the specified IP address of the sensor computer. The sensor processes the configuration package, uses it to generate a certificate signing request (CSR), and sends this request to the Server. After receiving the request, the Server web interface page displays the fingerprint of the received request as a sequence of characters. This same request fingerprint is also displayed on the sensor web interface page at the same time. You must make sure that these fingerprints are identical before completing the addition of the sensor.

  Adding and connecting a sensor automatically over the network ?

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
  2. Select **Settings** → **Deployment**.
  3. Click the **Add sensor** button.

     The details area appears in the right part of the web interface window.
  4. On the **Automatically over the network** tab:

     a. Enter the sensor name that will represent the sensor within Kaspersky Industrial CyberSecurity for Networks.

        The sensor name must be unique (not match the names of other sensors or the Server) and must contain no more than 100 characters. You can use letters of the English alphabet, numerals, a space, and the following special characters: `_` and `-` (for example, `Sensor_1`). The sensor name must begin and end with any permitted character except a space.

     b. Enter the Server IP address that the sensor will use to connect to the Server.

     c. Enter the IP address used by the web server on the sensor computer.
  5. Click the **Connect and add sensor** button.

     The application will establish a connection with the sensor computer, then the Server web interface page will show a prompt to confirm the received fingerprint for the certificate signing request.
  6. Connect to the sensor through the web interface.

     The sensor web interface page will show a message containing information about the certificate request fingerprint that was sent to the Server.
  7. Make sure that the sequences of characters representing the certificate request fingerprint are identical on the web interface pages of the sensor and Server.
  8. On the Server web interface page, click the button to confirm the received certificate request fingerprint.

  The sensor will connect to the Server, then information about the connection will be displayed on the Server and sensor web interface pages.

Creating a new communication data package for a sensor

If necessary, you can create a new communication data package for a sensor (for example, if you need to update the certificate used for connecting the sensor to the Server).

To create a new communication data package for a sensor:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the node tile of the sensor for which you want to create a new communication data package.

   The details area appears in the right part of the web interface window.

4. Click the **Get new communication data package** button. If the button is not displayed on the toolbar, click the ⋮ button and select the desired item in the menu that opens.

5. In the **Generating a new communication data package** window that opens:

   a. Enter the Server IP address that the sensor will use to connect to the Server.

   b. Enter password for protecting the certificate in the communication data package.

      The password must meet the following requirements:

      - Must contain between 8 and 256 ASCII characters.

      - Must contain one or more uppercase letters of the English alphabet.

      - Must contain one or more lowercase letters of the Latin alphabet.

      - Must contain one or more numerals.

      - Must contain no more than three consecutive repeated characters.

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

   The Server generates a new communication data package for the selected sensor, then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

7. On the sensor computer return the sensor to the initial state using the kics4net-reset-to-defaults.sh script that reverts the node to the initial state. The script is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

8. Connect to the sensor through the web interface.

9. On the sensor web interface page, upload the new communication data package.

   The new communication data package is uploaded the same way it is uploaded when adding a sensor using a communication data package.

Removing a sensor

To remove a sensor:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.
3. Select the node tile of the sensor that you want to delete.

   The details area appears in the right part of the web interface window.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, click **OK**.

Changing the main node settings

For the Server and the added sensors, you can change the following main settings:

- Settings for storing the application data on the node
- Node name
- Settings for using the external storage for traffic dump files

Changing the application data storage settings on a node

You can change the limits on the maximum space used for storing application data on a node.

To change the maximum space limits:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the tile of the relevant node.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the node parameters.
5. On the **General** tab, in the **Storage settings** section, define the maximum space limits for application data. The set of data types available for configuration depends on the type of node (Server or sensor).

   You can select the unit of measure for the space limit: **MB** or **GB**.

   For some data types (such as events), you can define a storage time limit in days.
6. Click **Save**.

Renaming a node that has application components installed

You can change the defined name of a node hosting the installed application component (Server or sensor).

To change the node name:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the tile of the relevant node.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.
5. In the field containing the current name of the node, enter a new name.

   The node name must be unique (must not match the names of other nodes) and must contain no more than 100 characters. You can use letters of the English alphabet, numerals, a space, and the special characters _ and - (for example, Server_1). The node name must begin and end with any permitted character except a space.
6. Click **Save**.

Connecting and configuring external storage for traffic dump files

The application saves traffic received through the monitoring points as traffic dump files. The application uses the internal storage of each node for online storage of files and analysis of traffic saved in these files. The application saves and deletes files in the internal storage in accordance with the internal storage settings specified for the node. Connect and configure the external storage on the node to ensure long-term storage of the traffic dump files. Traffic dump files stored in the external storage can be used to download traffic to PCAP files, for example, to download traffic from the network sessions if the dump files of this traffic are already deleted from the internal storage on the node.

Use a directory in the local file system of the node computer as the external storage. This directory must be mounted on a hard drive having sufficient free space and not containing the /var/ directory. For external storage, you can also use a directory where a shared network resource of another computer is mounted, for example, a directory similar to the directory for exporting events to a network resource. A directory in the local file system must be granted permissions for the kics4net account, including the permissions to create nested directories.

Actions for creating and mounting a directory for the external storage are performed using the standard operating system tools of the node computer.

To connect and configure the external storage for the traffic dump files on a node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the tile of the relevant node.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the node parameters.

5. Select the **External storage** tab and enable the external storage usage mode by the **Connect external storage for traffic dump files** switch.
6. Specify the path in the local file system of the node to the directory intended for external storage.
7. Set the space limit for storing the traffic dump files in the **Maximum size** group of settings.

   You can select the unit of measure for the space limit: **MB** or **GB**.
8. If necessary, in the **Filtering stored traffic** section, enable filtering and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

   > Filtering reduces the volume of the stored traffic by skipping the network packets that do not match the filter. However, in this case, when you later view the traffic dump files or download traffic from these files, you are not able to download the network packets skipped when the traffic was saved.
9. If necessary, in the **Storage time limit** section, enable a limit on the minimum storage time for the files and specify the required number of days.
10. Click **Save**.

Managing monitoring points on nodes

Monitoring points are used for receiving and processing industrial network traffic in Kaspersky Industrial CyberSecurity for Networks. Monitoring points can be added or removed on any node that has application components installed (including on a node that performs Server functions). When adding or removing them, you do not need to restart the computer on which the application components are installed or reinstall components on the computer.

Each monitoring point must be associated with a network interface that receives a copy of traffic from a specific industrial network segment. To add monitoring points, you can use network interfaces that meet the following conditions:

- Type of network interface: Ethernet.
- MAC address: different from 00:00:00:00:00:00.
- The network interface is intended for receiving a copy of industrial network traffic, and this network interface is not used for other purposes (for example, to connect nodes that have application components installed).

You can add monitoring points to not only physical network interfaces but also to logical interfaces that combine multiple physical interfaces (bonded interfaces). However, you cannot add a monitoring point to a physical network interface that is one of the interfaces of a logical bonded interface.

Monitoring points can be enabled and disabled. You can disable a monitoring point to temporarily stop monitoring an industrial network segment relaying a copy of traffic to a network interface. When you need to resume monitoring of the industrial network segment, you can enable the monitoring point.

> After disabling or removing a monitoring point, the application may still register events associated with this monitoring point for some time. This is due to a possible delay in processing incoming traffic when the Server is experiencing high loads.

Adding a monitoring point

To receive and process traffic flowing from the industrial network to the network interface of a node, you need to add a monitoring point to this network interface.

Only users with the Administrator role can add monitoring points to network interfaces.

To add a monitoring point to a network interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Open the details area by clicking the **Add monitoring point** link in the tile of the relevant network interface. The link is displayed if a monitoring point has not been added to the network interface.

   The details area appears in the right part of the web interface window.

4. In the entry field in the upper part of the details area, enter the name of the monitoring point.

   You can use uppercase and lowercase letters of the English alphabet, numerals, and the `_` and `-` characters.

   The monitoring point name must meet the following requirements:

   - Must be unique (not assigned to another monitoring point).

   - Must contain from 1 to 100 characters.

5. Click the **Add monitoring point** button.

Enabling monitoring points

The application does not receive and does not process traffic transmitted through the network interface of a disabled monitoring point. You need to enable the monitoring point if you want to resume receiving and processing traffic.

You can enable monitoring points individually, or all of them on one node or all nodes simultaneously.

Only users with the Administrator role can enable monitoring points.

To enable monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Do one of the following:

   - If you want to enable one monitoring point, click the **Enable** button in the network interface tile containing the monitoring point. The button is available if the monitoring point is disabled.

- If you want to enable all monitoring points on a node, click the **Enable all** button in the node tile hosting the disabled monitoring points. The button is available if the node has network interfaces with disabled monitoring points.

- If you want to enable all monitoring points on all nodes, use the **Enable on all nodes** link in the toolbar.

4. Wait for the changes to be applied.

Disabling monitoring points

You can disable a monitoring point if you need to temporarily pause the receipt and processing of traffic on the network interface of this monitoring point.

You can disable monitoring points individually, or all of them on one node or all nodes simultaneously.

Only users with the Administrator role can disable monitoring points.

To disable monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Do one of the following:

   - If you want to disable one monitoring point, click the **Disable** button in the network interface tile containing the monitoring point. The button is available if the monitoring point is enabled.

   - If you want to disable all monitoring points on a node, click the **Disable all** button in the node tile hosting the enabled monitoring points. The button is available if the node has network interfaces with enabled monitoring points.

   - If you want to disable all monitoring points on all nodes, use the **Disable on all nodes** link in the toolbar.

4. Wait for the changes to be applied.

Renaming a monitoring point

You can rename a monitoring point linked to a network interface.

> The new name of the monitoring point will appear in events that are registered after its renaming. The old name of the monitoring point is displayed in previously registered events.

Only users with the Administrator role can rename a monitoring point.

To rename a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the network interface tile containing the monitoring point that you want to rename.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button and enter a new name in the field that appears.

   You can use uppercase and lowercase letters of the English alphabet, numerals, and the _ and - characters.

   The monitoring point name must meet the following requirements:

   - Must be unique (not assigned to another monitoring point).
   - Must contain from 1 to 100 characters.

5. Click **Save**.

Deleting a monitoring point

You can delete a monitoring point linked to a network interface. Deletion of a monitoring point may be required if this network interface will no longer be used for receiving industrial network traffic.

If it becomes necessary to temporary pause the receipt of traffic at a network interface of a monitoring point (for example, while performing preventative maintenance and adjustment operations), you can disable the monitoring point without deleting it.

> The traffic received from a monitoring point prior to its deletion is not deleted from the database. Information about this monitoring point is also saved in the table of registered events.

Only users with the Administrator role can delete a monitoring point.

To remove a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the network interface tile containing the monitoring point that you want to delete.

   The details area appears in the right part of the web interface window.

4. In the details area, click **Remove**.

   A window with a confirmation prompt opens. If the monitoring point is enabled, the application will prompt you to disable the monitoring point.

5. In the prompt window, confirm deletion of the monitoring point.

Identifying the Ethernet port associated with a network interface

A computer on which application components are installed may have multiple Ethernet ports used for connecting to the local area network. You can use the application to enable blink mode for a network interface and identify which Ethernet port is associated with this interface. When blink mode is enabled, the LED indicator next to the Ethernet port blinks for 15 seconds.

If the network interface does not support LED blink mode (for example, there is no LED indicator next to the Ethernet port or the network interface is a logical bonded interface), an error occurs when blink mode is enabled.

Only users with the Administrator role can enable Ethernet port blink mode.

To determine which Ethernet port is linked to a network interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Click the **Blink** button on the network interface tile.

   If the network interface supports an LED indicator, the network cable connection icon begins to blink on the network interface tile. At the same time, the LED indicator next to the Ethernet port begins to blink on the corresponding network adapter of the computer.

While blink mode is enabled for one network interface, you cannot enable blink mode for another network interface on the same node.

Managing technologies

Kaspersky Industrial CyberSecurity for Networks uses various technologies to analyze industrial network traffic. You can enable or disable the use of individual technologies. For some technologies, you can select the operation mode: learning mode or monitoring mode.

It is recommended to enable the technology learning mode for a predefined time so that the application automatically switches technologies to the monitoring mode at the right moment. The monitoring mode is a standard technology operation mode (as opposed to the learning mode, when the application only accumulates data for further use). When configuring the learning mode, you can set the desired time for the technology to automatically switch to the monitoring mode.

You can configure the same technology usage settings on all nodes and monitoring points or configure specific settings for the desired nodes and monitoring points. Technology usage settings can be automatically inherited from parent objects to child objects. If technology inheritance is enabled for a node or a monitoring point, the technology usage settings configured for the parent object (Server or sensor) are applied to this object. If technology inheritance is disabled, you can configure specific technology usage settings on this node or monitoring point.

After the application is installed, all technologies except for PLC Project Control and Unknown Tag Detection are enabled by default. The learning mode is enabled by default for the technologies that support mode change. When adding sensors and monitoring points to the application, the inheritance of technologies set for the parent object is enabled for them by default.

Enabling and disabling technologies

You can enable or disable the use of technologies for the Server, sensors, and monitoring points. Enabling or disabling technologies on sensors and monitoring points is available if technology inheritance is disabled for these objects.

Some technologies include methods that can be enabled or disabled separately. If a technology or method is disabled, the application does not monitor communications of devices using this technology or method. You can configure the application settings related to the disabled technologies or methods (for example, add or edit rules).

The following technologies and methods can be enabled and disabled:

- Asset Management:
  - Device activity detection
  - Device Information Detection
  - PLC Project Control
  - Network Session Detection.
  - Risk detection (only on the Server node)
- Network Control:
  - Network Integrity Control
  - Command Control
- Process Control:
  - Rule-based Process Control
  - Unknown Tag Detection
  - Device Discovery for Process Control
- Intrusion Detection:
  - Rule-based Intrusion Detection
  - ARP Spoofing Detection
  - IP Protocol Anomaly Detection
  - TCP Protocol Anomaly Detection
  - Brute-force Attack and Scan Detection

This article describes the procedure of enabling and disabling technologies on a Server node. The actions for enabling or disabling technologies on sensor nodes and monitoring points are performed in the same way after the technology inheritance is disabled for these objects.

To change the state of technologies and methods on the Server node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the Server tile.

   The details area appears in the right part of the web interface window. The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled.

   > If the states of technologies and methods cannot be currently changed, the switches in the list are disabled. In this case, it is recommended to check the status of the kics4net service on the Server computer. If the service is not active, you must start it.

4. Use the toggle switches on the left to enable or disable the use of relevant technologies and/or methods. You can enable or disable all technologies and methods simultaneously by clicking the **Enable all** or **Disable all** links.

5. After enabling or disabling a technology or method, wait for the changes to be applied. The toggle switch is unavailable until it is finished moving to the other state.

Configuring technology operating modes

You can configure the technology learning mode or manually enable the monitoring mode for the Server, sensors, and monitoring points. These actions are available on sensors and monitoring points if technology inheritance is disabled for these objects.

The mode can be changed for the following technologies and methods:

- Device activity detection
- Command Control
- Rule-based Process Control
- Network Integrity Control

This section describes the procedure of changing and configuring technology modes on a Server node. The actions for changing and configuring technology modes on sensor nodes and monitoring points are performed in the same way after the technology inheritance is disabled.

To change and configure the modes of technologies and methods on the Server node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the Server tile.

   The details area appears in the right part of the web interface window. The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled.

   > If the operation modes of technologies and methods cannot be currently changed, the switches in the list are disabled. In this case, it is recommended to check the status of the kics4net service on the Server computer. If the service is not active, you must start it.

4. For the technologies and methods that support operation in the learning mode, in the drop-down list to the right of the technology or method name, select the required mode (**Learning** or **Monitoring**). If you want to select the same mode for all these technologies and methods, use the **Mode** drop-down list.

   If different modes are selected, the **Mode** drop-down list displays the **Mixed** value.

5. After selecting a mode, wait for the changes to be applied. Until the mode is applied, the drop-down list displays the *Changing* status.

6. For the technologies and methods operating in the learning mode, specify the date and time when they automatically switch to the monitoring mode. For this purpose, click the **Set until** link and select the date and time. If the date and time are configured before, they are displayed next to the mode name.

Managing inheritance of technologies

If you want a sensor or a monitoring point to automatically get the technology usage settings configured for a parent object, you can enable technology inheritance. In this case, the sensor gets the technology usage settings defined for the Server, and the monitoring point gets the settings defined for the node for which the monitoring point is added (for the Server or a sensor).

If necessary, you can disable technology inheritance on a sensor or monitoring point. This allows you to configure specific technology usage settings for this object.

To enable or disable technology inheritance on a sensor node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the sensor tile.

   The details area appears in the right part of the web interface window.

4. Set the **Inherit Server technologies** switch to the desired position.

To enable or disable technology inheritance on a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the network interface tile with the monitoring point for which you want to enable or disable technology inheritance.

   The details area appears in the right part of the web interface window.

4. Set the technology inheritance switch to the desired position.

Downloading traffic received by the node monitoring points

You can download traffic received by the application through monitoring points on nodes. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads traffic from the traffic dump file storages. Both the internal storage of each node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

When downloading traffic, take the following considerations into account:

- Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.
- Only the users with the Administrator role can download traffic received by node monitoring points.

To download traffic received by the node monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Do one of the following:
   - To download traffic received by the monitoring points of a certain node, select the tile of this node.
   - To download traffic received by a specific monitoring point, select the network interface card with this monitoring point.

   The details area appears in the right part of the web interface window.
4. Click the **Download traffic** button. If the button is not displayed on the toolbar, click the ⋮ button and select the desired item in the menu that opens.
5. Do the following in the opened window:
   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

     The default period is one hour.
   - Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

     If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.
   - When a node tile is selected, if necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points of the node that receives the necessary traffic (this section is displayed if a node tile is selected).

     By default, all monitoring points available on the selected node are specified.
   - If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets belong (this section is displayed if additional address spaces are added to the application).

     By default, all address spaces created in the application are specified.
   - If necessary, enable filtering in the **BPF filtering** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

Filtering expression example:
`tcp port 102 or tcp port 502`

- If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets.

  Filtering expression example:
  `^ test. + xABxCD`

6. Click the **Show** button.

7. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the ⤓ button in the menu of the application web interface.

   The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Monitoring the state of Kaspersky Industrial CyberSecurity for Networks

This section contains instructions on monitoring the state of the application.

Monitoring the application state when connected through the web interface

You can view information about the current state of the application when connected to the Server through the web interface. The application state is monitored by using the corresponding widgets in the **Dashboard** section.

The application also informs about disabled protection functions and operational issues.

Information about disabled protection functions

If some protection functions are disabled, the **Not all protection services are running** notification is displayed in the lower part of the menu on the application web interface page. The notification is displayed in the following cases:

- One or more monitoring points are disabled.
- One or more protection functions are disabled (for example, rule-based Intrusion Detection).
- Learning mode is enabled for one or multiple protection functions (for example, for Network Integrity Control technology).

To view information about disabled protection functions:

1. Click the **Not all protection services are running** notification.

   The **Components not providing protection** window opens.

2. Select one of the following tabs:

   - **Server** – to view information about the disabled Server protection functions.

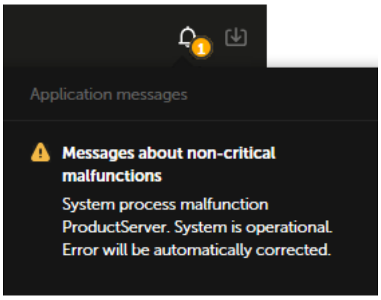
     If technology inheritance is enabled on the nodes of the sensors and monitoring points, the **Inheritance of technologies on all components is enabled** message is displayed in the upper right corner of the **Sensor** tab.

   - **Sensors** – to view information about the disabled sensor protection functions.

   - **Monitoring points** – to view information about the disabled monitoring points' protection functions.

Notifications about application operation problems

The upper part of the web interface menu contains a button for opening the list of notifications about problems in application operation (see the figure below).



Application messages

Messages about non-critical malfunctions

System process malfunction ProductServer. System is operational. Error will be automatically corrected.

List of notifications about problems in application operation in the browser window

If the list contains notifications about critical problems (for example, messages about disruption of application operation), a red icon is displayed. If the list contains only notifications about non-critical problems, a yellow icon is displayed.

The list contains only up-to-date notifications. If a problem has been resolved (for example, a lost connection with the Server has been restored), the corresponding notification is automatically removed from the list.

You can view detailed information about notifications (except notifications regarding unavailability of the Server or database).

To view information about a notification:

1. In the menu, click the 🔔 button.

2. In the list of notifications, click the text of the notification.

   The browser window will show the section containing information pertaining to the notification (for example, under **Settings** → **Application messages**).

Viewing application messages

The application message log stores information about errors in application operation and about errors in operations performed by system processes of Kaspersky Industrial CyberSecurity for Networks.

You can view application messages when connected to the Server through the web interface. If necessary, you can also configure forwarding of application messages to recipient systems via connectors.

To view application messages:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Application messages**.

   The table will display application messages that match the defined filter and search settings.

The settings of application messages are displayed in the following columns of the table:

- **Date and time**

  Date and time when the application message was registered.
- **Status**

  Status of the message. The following statuses are available for messages:
  - *Normal operation* – for informational messages.
  - *Unknown*, *Malfunction* – for messages about non-critical malfunctions in application operation.
  - *Moderate malfunction, Critical malfunction*, *Fatal malfunction* – for messages about disruption of application operation.
- **Node**

  Name or IP address of the node from which the message originated.
- **System process**

  Application process that invoked message registration.
- **Message**

  Numerical identifier and text of the message.

When viewing the application messages table, you can use the filter, search, and sorting functions.

Viewing user activity audit entries

Kaspersky Industrial CyberSecurity for Networks can save information about actions performed by users in the application. Information is saved in the audit log if user activity audit is enabled.

You can view audit entries when connected to the Server through the web interface. If necessary, you can also configure the forwarding of audit entries to recipient systems via connectors.

Only users with the Administrator role can view audit entries.

To view audit entries:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Audit**.

   The table will display the audit entries that match the defined filter and search settings.

The settings of audit entries are displayed in the following columns of the table:

- **Date and time**

  Date and time when the user action data was registered.

- **Action**

  Registered action performed by the user.

- **Result**

  Result of the registered action (successful or unsuccessful).

- **User**

  Name of the user that performed the registered action.

- **User node**

  IP address of the node where the registered action was performed.

- **Description**

  Additional information about the registered action.

When viewing the audit entries table, you can use the configuration, filter, search, and sorting functions.

Viewing information about nodes with application components installed and about network interfaces on nodes

Users with the Administrator role and users with the Operator role can both view information about nodes with application components installed and about network interfaces on nodes.

To view information about nodes and network interfaces:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Deployment**.

   The web interface window displays node tiles (on the left) and network interface tiles detected on these nodes (on the right of each node).
3. If you want to view detailed information about a node or network interface, select the tile of the relevant node or network interface.

   The details area appears in the right part of the web interface window.

Displayed information about nodes with application components installed

A node tile displays the following information:

- Current node status.

    - ✓ *OK*. The node is available, and no application messages about non-critical malfunctions or disrupted operation were received from this node.

    - ⚠ *Non-critical malfunction*. The node is available, and application messages with the *Unknown* or *Malfunction* status were received from it.

    - ! *Operation disrupted*. The node is available, and application messages with the *Moderate malfunction*, *Critical malfunction* or *Fatal malfunction* status were received from this node.

    - ? *No connection*. The node is unavailable.

- Node name.

- Application component installed on the node: **Server** or **Sensor**.

- IP address for connecting to the node (address 0.0.0.0 corresponds to all possible IP addresses on the computer).

- The current mode of the technologies for which the operating mode can be selected. The tile contains the name of the mode: *Learning* or *Monitoring*, if all technologies operate in this mode. If different modes are selected for the technologies, the *Mixed* value is displayed.

- If the inheritance of Server technologies is disabled for a sensor, the 🔄 icon is displayed.

How to view the node information in the details area ?

The details area displays the following information for the selected node:

- Node name.
- The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled on the node.

  For the technologies with a selectable operating mode, the current mode is displayed: **Learning** or **Monitoring**. If learning mode is enabled, the date and time of the automatic switching to the monitoring mode are displayed to the right of the mode name (the date and time are not displayed if the time of the automatic switching is not set).
- The following information is displayed on the **Settings** tab:
  - **Status** – current status of the node indicated by an icon and text description (like in the node tile).
  - **Node type** – application component installed on the node: **Server** or **Sensor**.
  - **Disk space currently used by the application** – disk space occupied by application files. This includes the installed files and files that are created while the application is running.
  - **Maximum disk space that can be used by the application** – disk space that can be occupied by application files. This includes the installed files and the sum of all volume limits defined in data storage rules. This value cannot exceed the available disk space.
  - **Occupied on disk** – disk space used by all files. This includes application files and files of the operating system and other applications. This volume of space is calculated on the drive that contains the /var/ folder in the file system of the node.
  - **Free disk space** – disk space that is not used by files. This volume of space is calculated on the drive that contains the /var/ folder in the file system of the node.
  - **Total disk space** – total volume of disk space on the drive that contains the /var/ folder in the file system of the node.
  - **Inheritance of technologies**—a flag indicating if the inheritance of Server technologies is enabled or disabled (only for the sensor node).
  - **Retention rules**—current and maximum values of the following settings: volume, number of items, and storage time of the application data.

Displayed information about network interfaces

A network interface tile displays the following information:

- Icon showing if a network cable is connected to the Ethernet port of the network interface:
  - 🟢 – the network cable is connected.
  - ⚪ – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.
- Network interface name in the operating system.

- MAC address.
- Rate of incoming traffic received by the network interface.
- Information about the monitoring point (if one was added):
  - Current status of the monitoring point:
    - ✓ *OK*. The monitoring point is available.
    - ⚠ *Switchover*. The operating mode of the monitoring point is being changed.
    - ! *Error*. An error was detected when switching over the operating mode of the monitoring point.
  - Monitoring point name.
  - Current operating mode of the monitoring point:
    - If the monitoring point is disabled, the *Disabled* value is displayed.
    - If the monitoring point is enabled, the current mode of the technologies for which the operating mode can be selected is displayed. The tile contains the name of the mode: *Learning* or *Monitoring*, if all technologies operate in this mode. If different modes are selected for the technologies, the *Mixed* value is displayed.
  - If the inheritance of the node technologies is disabled for a monitoring point, the 🔄 icon is displayed.

How to view the network interface information in the details area ?

For a network interface to which a monitoring point is not added, the following information is displayed in the details area:

- **Network interface** – name of the network interface in the operating system.
- **Connection** – icon indicating that a network cable is connected to the Ethernet port of the network interface:
  - ● – the network cable is connected.
  - ○ – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.
- **MAC address** – MAC address of the network interface.
- **IP address** – IP address of the network interface. If multiple IP addresses are detected on a network interface, the details area displays no more than 16 IP addresses.

If a monitoring point has been added to the network interface, the following information is displayed:

- Monitoring point name.
- **Status** – current status of the monitoring point indicated by an icon and text description:
  - ✓ *OK*. The monitoring point is available.
  - ⚠ *Switchover*. The operating mode of the monitoring point is being changed.
  - ❗ *Error*. An error was detected when switching over the operating mode of the monitoring point.
- **Network interface** – name of the network interface in the operating system.
- **Mode** – current operating mode of the monitoring point:
  - *Enabled*.
  - *Disabled*.
- The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled on the monitoring point.

  For the technologies with a selectable operating mode, the current mode is displayed: **Learning** or **Monitoring**. If learning mode is enabled, the date and time of the automatic switching to the monitoring mode are displayed to the right of the mode name (the date and time are not displayed if the time of the automatic switching is not set).
- On the **Settings** tab:
  - **Inheritance of technologies**—a flag indicating if the inheritance of the node technologies is enabled or disabled.
  - **MAC address** – MAC address of the network interface.
  - **IP address** – IP address of the network interface. If multiple IP addresses are detected on a network interface, the details area displays no more than 16 IP addresses.

Viewing the status of services supporting operation of application components

You can view the status of services that support the operation of application components. If the service is active, this means that it was successfully started.

To view the status of a service:

1. On the computer on which the application component is installed, open the operating system console.
2. Enter the following command:

   ```
   sudo service <service name> status
   ```

   where `<service name>` is the name of the service, whose information you want to view. You can specify the following services:

   - `kics4net` – main service (runs only on a computer that performs Server functions).
   - `kics4net-apm` – active polling connector service (runs on a computer that performs Server or sensor functions).
   - `kics4net-asset-inventory` – service for processing the results of scanning device attributes using OVAL rules (runs only on a computer that performs Server functions).
   - `kics4net-blob-storage` – service for storing arrays of binary data (runs only on a computer that performs Server functions).
   - `kics4net-connectors-launcher` – registration and launch of manageable connectors service (runs on a computer that performs Server functions or sensor functions)
   - `kics4net-email-gateway` – service for sending email notifications (runs only on a computer that performs Server functions).
   - `kics4net-epp-proxy` – Kaspersky Endpoint Agent integration service (runs on a computer that performs Server functions or sensor functions).
   - `kics4net-fts` – full-text search system service (runs only on a computer that performs Server functions).
   - `kics4net-nats-server` – message broker service (runs on a computer that performs Server functions or sensor functions).
   - `kics4net-oval-facade` – service for scanning remote devices using OVAL rules (runs on a computer that performs Server or sensor functions).
   - `kics4net-postgresql` – DBMS service (runs only on a computer that performs Server functions)
   - `kics4net-report-builder` – service for generating reports (runs only on a computer that performs Server functions).
   - `kics4net-report-data-source` – service for providing data for reports (runs only on the computer that performs Server functions)

- `kics4net-report-renderer` –service for visual display of data blocks in the reports (runs only on the computer that performs Server functions)

- `kics4net-report-templates-catalog` – service for managing report templates (runs only on the computer that performs Server functions)

- `kics4net-report-templates-catalog-view` – service for providing data about the report templates (runs only on the computer that performs Server functions)

- `kics4net-responses-manager` – service for managing the response jobs (runs only on the computer that performs Server functions)

- `kics4net-risk-oval-detector` – service for processing the results of device scan for risks using the OVAL rules (runs only on the computer that performs Server functions)

- `kics4net-scan-oval-manager` – service for managing device scanning using OVAL rules (runs only on the computer that performs Server functions)

- `kics4net-scap-manager` – service for managing security audit (runs only on the computer that performs Server functions)

- `kics4net-scap-manager-view` – service for providing security audit data (runs only on the computer that performs Server functions)

- `kics4net-scheduler` – task scheduling service (runs only on a computer that performs Server functions).

- `kics4net-secrets` – service for the secrets repository facade (runs only on the computer that performs Server functions)

- `kics4net-task-manager` – task management service (runs only on a computer that performs Server functions)

- `kics4net-task-manager-view` – service for providing data about tasks (runs only on the computer that performs Server functions)

- `kics4net-vault` – service for storing secrets in the repository (runs only on the computer that performs Server functions)

- `kics4net-websensor` – web server service (runs only on a computer that performs sensor functions).

- `kics4net-webserver` – web server service (runs only on a computer that performs Server functions).

- `klnagent` –Network Agent service (runs only on a computer that performs Server functions).

  Example:

  ```
  sudo service kics4net status
  ```

If the service is not active, you can restart the computer or restart the service.

Restarting a computer that has application components installed

When restarting a computer that performs Server or sensor functions, application components are automatically started. A restart does not affect the subsequent operation of these components (except in some situations when there is a malfunction after an unexpected restart).

A restart may be required in the following cases:

- There is not enough free space on the computer hard drive.
- The computer was unexpectedly restarted, after which the operation of application components was not restored.
- One of the application services is not active.
- A lost connection between the Server and a sensor is not being restored. In this case, you should restart the computer that performs sensor functions.

You can use the standard commands of the operating system to restart a computer that has application components installed.

If the computer cannot be restarted for some reason, you can restart the services that support operation of application components.

To restart services:

1. Open the operating system console.
2. Depending on which functions are performed by the computer, do the following:
   - If the computer performs Server functions, enter the following sequence of commands:

```
sudo service kics4net-postgresql restart
sudo service kics4net-nats-server restart
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-oval-facade restart
sudo service kics4net-asset-inventory restart
sudo service kics4net-blob-storage restart
sudo service kics4net-email-gateway restart
sudo service kics4net-fts restart
sudo service kics4net-report-builder restart
sudo service kics4net-report-data-source restart
sudo service kics4net-report-renderer restart
sudo service kics4net-report-templates-catalog restart
sudo service kics4net-report-templates-catalog-view restart
sudo service kics4net-responses-manager restart
sudo service kics4net-risk-oval-detector restart
sudo service kics4net-scap-manager restart
sudo service kics4net-scap-manager-view restart
sudo service kics4net-scan-oval-manager restart
sudo service kics4net-scheduler restart
sudo service kics4net-vault restart
sudo service kics4net-secrets restart
sudo service kics4net-task-manager restart
sudo service kics4net-task-manager-view restart
sudo service kics4net-webserver restart
sudo service klnagent restart
```

- If the computer performs sensor functions, enter the following sequence of commands:

```
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
sudo service kics4net-websensor restart
```

Using a test network packet to verify event registration

To verify the registration of events in Kaspersky Industrial CyberSecurity for Networks, you can use a test network packet. When this type of packet is detected in traffic, the application registers test events based on the following technologies:

- Deep Packet Inspection An event is registered regardless of whether or not there are Process Control rules or tags.

- Network Integrity Control An event is registered regardless of whether or not there are Interaction Control rules. Use of Network Integrity Control technology must be enabled.

- Intrusion Detection An event is registered regardless of whether or not there are Intrusion Detection rules. Use of Rule-based Intrusion Detection must be enabled.

- Asset Management An event is registered regardless of whether or not there are known devices in the devices table. Use of device activity detection must be enabled.

Events are registered with system event types that are assigned the following codes:

- 4000000001 for an event based on Deep Packet Inspection technology.

- 4000000002 for an event based on Network Integrity Control technology.

- 4000000003 for an event based on Intrusion Detection technology.

- 4000000004 for an event based on Asset Management technology.

You can view test events in the table of registered events.

To verify audit functions, Kaspersky Industrial CyberSecurity for Networks saves information about the registration of test events in the audit log. An audit entry is created for each registered event, and this entry specifies the technology used to register the test event.

A test network packet is a UDP protocol packet with certain parameter values. The parameters are defined in such a way as to exclude the probability of receiving such a packet in normal industrial network traffic.

The following data must be defined in the parameters of a test network packet:

- Ethernet II header:
  - Source MAC address: `00:00:00:00:00:00`
  - Destination MAC address: `ff:ff:ff:ff:ff:ff`
  - EtherType: `0x0800 (IPv4)`
- IP header:
  - Source IP address: `127.0.20.20`
  - Destination IP address: `127.0.20.20`
  - ID: `20`
  - TTL: `20`
  - Protocol type: `17 (UDP)`
  - Flags: `0x00`
- UDP header:
  - Source port: `20`
  - Destination port: `20`
- Packet contents:
  - Length of packet contents, in bytes: `20`
  - Packet contents: `"KICS4Net Sentinel 20"`

To generate and send a test network packet, you can use a network packet generator program such as Scapy. You need to send the test network packet from a node whose traffic is controlled by Kaspersky Industrial CyberSecurity for Networks.

Example:

To send a test network packet using the program Scapy in a Linux® operating system:

1. In the operating system console of the computer, enter the command to run Scapy in interactive mode:

   ```
   sudo scapy
   ```

2. Enter the command to send the test network packet:

   ```
   sendp(
   Ether(src='00:00:00:00:00:00', dst='ff:ff:ff:ff:ff:ff')/
   IP(src='127.0.20.20', dst='127.0.20.20', id=20, ttl=20)/
   UDP(sport=20, dport=20)/
   "KICS4Net Sentinel 20",
   iface="<interface name>"
   )
   ```

   where <`interface name`> is the name of the network interface connected to the industrial network (for example, `eth0`).

After the packet is detected in traffic, Kaspersky Industrial CyberSecurity for Networks registers test events.

Checking the integrity of application modules

You can check the integrity of installed software modules to make sure that there were no changes to those modules after installation. This check is performed by comparing the checksums of installed application modules with their reference values. An integrity check must be run separately on each node hosting installed application modules.

You can run an integrity check on a node in the following ways:

- Run the check locally using the kics4net-manifest-checker-<application version>.bundle.sh script.
- Run when connecting to the Server through the web interface.

Running an integrity check locally using a script

The kics4net-manifest-checker-<application version>.bundle.sh script is included in the Kaspersky Industrial CyberSecurity for Networks distribution kit. The script checks the application module files against special lists that are stored in the *manifest files*. The manifest files are included in the application installation packages and contain file lists of the corresponding packages. Each application package has a corresponding manifest file. The manifest files are digitally signed and their integrity is also verified.

> If you make any changes to the kics4net-manifest-checker-<application version number>.bundle.sh script file, its results may be invalid. For valid results, use only that version of the script which is include in the Kaspersky Industrial CyberSecurity for Networks distribution kit.

While running, the script sequentially checks the checksums of files from the application packages installed in the operating system.

To check the integrity of application modules on a node computer by using the kics4net-manifest-checker-<application version>.bundle.sh script:

1. Copy to any folder the script file kics4net-manifest-checker-<application version number>.bundle.sh from the folder with unpacked script files and packages for installing, validating and removing application components, contained in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.
2. In the operating system console, go to the folder containing the script file, and enter the following command:
   ```
   sudo bash kics4net-manifest-checker-< application version >.bundle.sh
   ```

Information about the results of the check are displayed in the operating system console.

The results of the software module integrity check on the computer are considered successful if the following two conditions are met:

- The kics4net-manifest-checker-<application version number>.bundle.sh script terminates with the message: `All files of installed packages containing the manifest file have been successfully checked.`
- All application packages that should be installed on the computer in accordance with their proper functions do not return error messages or at least do not return either of the following messages:

- `The package is not installed in the operating system.`
- `The manifest file for the package could not be found.`

Running an integrity check when connected to the Server through the web interface

You can run an integrity check of application modules on a node when connected to the Server through the web interface. An integrity check started in this way is performed using similar methods as the kics4net-manifest-checker-<application version>.bundle.sh script.

To check the integrity of application modules on a node computer when connected to the Server through the web interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the tile of the relevant node.

   The details area appears in the right part of the web interface window.

4. Click **Check integrity**. If the button is not displayed on the toolbar, click the ⋮ button and select the desired item in the menu that opens.

   You will see a message informing you that an integrity check was started, and information about its progress will be available in the list of background operations for some time. If necessary, you can view the current list of background operations by clicking the ▣ button in the application web interface menu.

5. To view the integrity check results, go to **Settings** → **Application messages**.

The results of an integrity check of application modules on a computer are deemed successful if the list of application messages includes the following message for the corresponding node: `Integrity check of application modules on node completed successfully`.

If the list of application messages does not include a message indicating a successful integrity check but instead contains an error message, the integrity check is deemed unsuccessful. You can identify the application packages that did not pass the integrity check by using the kics4net-manifest-checker-<application version>.bundle.sh script (see above).

Synchronizing the time on nodes of Kaspersky Industrial CyberSecurity for Networks with the time source used for industrial network devices

To correctly correlate the time of registration of events with the time when events occurred in the industrial network, time must be synchronized in the system. The time on nodes with Kaspersky Industrial CyberSecurity for Networks components installed must be synchronized with a common source of time used by industrial network devices.

When centrally installing Kaspersky Industrial CyberSecurity for Networks, you can enable automatic time synchronization between the Server and nodes where sensors are installed. In this case, the node with the Server installed will serve as the time source for nodes that have sensors installed. It is recommended to use the software tools from the operating system of the computer performing Server functions to configure time synchronization between the Server and the common time source used by devices in the industrial network. For Server time synchronization, you can use the standard protocols known as Network Time Protocol (NTP) and Precision Time Protocol (PTP).

NTP is used for automatic time synchronization between the Server and other nodes. In this case, you cannot configure synchronization with other time sources or use the PTP protocol on nodes that have sensors installed.

If a sensor was installed locally using the kics4net-install.sh script, automatic time synchronization with the Server is not performed on this node. If this is the case, you must configure time synchronization on the Server and on all nodes containing sensors that were installed locally.

For example sequences of operations for configuring time synchronization, please refer to the Appendices.

Updating SSL connection certificates

Kaspersky Industrial CyberSecurity for Networks can use the following certificates:

- Certificates for connections between nodes of Kaspersky Industrial CyberSecurity for Networks.
- Certificates for connecting to Kaspersky Industrial CyberSecurity for Networks through the web interface.
- Certificates for connecting through the Kaspersky Industrial CyberSecurity for Networks API.
- Certificates for connecting connectors.
- Certificates for connections with Kaspersky Endpoint Agent.

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 at the enterprise.

Updating certificates for connections between nodes of Kaspersky Industrial CyberSecurity for Networks

During installation of Kaspersky Industrial CyberSecurity for Networks, certificates for connections between nodes of Kaspersky Industrial CyberSecurity for Networks are automatically updated. You can manually update these certificates without reinstalling application components.

To update certificates for connections between nodes of Kaspersky Industrial CyberSecurity for Networks:

1. On the Server computer, go to the /opt/kaspersky/kics4net/sbin/ folder and enter the command to launch the script for local certificate update:

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. After the script finishes, return all sensors to the initial state using the kics4net-reset-to-defaults.sh script that reverts the node to the initial state. The script is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

3. Add and connect sensors again.

Updating the certificate for connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface

To update the certificate for connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface, you need to replace the certificate used by the web server. You can specify a new web server certificate under **Settings** → **Connection Servers** on the **Web Server** tab.

Updating the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API

To update the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API, you need to replace the certificate used by the REST API server. You can specify a new REST API server certificate under **Settings** → **Connection Servers** on the **REST API server** tab.

Updating certificates for connecting connectors

You can update certificates for connecting unmanageable connectors (or connectors configured to ignore the functions of a manageable connector) when creating new communication data packages for connectors. To update the certificates of manageable connectors, you must remove these connectors and then add them again.

Updating certificates for connections with Kaspersky Endpoint Agent

You can update the certificates used for connections with Kaspersky Endpoint Agent when changing the settings of integration servers.

Updating databases and application modules

Kaspersky Industrial CyberSecurity for Networks provides the capability to update the following databases and application modules:

- System Intrusion Detection rules.
- Modules for processing application-layer protocols for industrial process control purposes.
- Event correlation rules for registering incidents.
- Rules for obtaining information about devices and communication protocols.
- Industrial equipment vulnerabilities database.
- Kaspersky Digital Signature (KDS) certificate revocation list.
- Application functionality configuration.
- Security audit system rules.
- OpenSSL cryptographic module.
- Kaspersky ICS CERT vulnerabilities database for SCADA.

- Methods for identifying techniques of potential attacks based on system command detection events.

Application modules and databases are updated after installing updates released by Kaspersky.

> Timely installation of updates ensures maximum protection of an industrial network using Kaspersky Industrial CyberSecurity for Networks. In addition, these updates can augment and update application modules involved in providing security for the application. Failure to regularly install updates over time will increase the risks to application security due to the emergence of new threats. You must also install security updates for your particular operating system.

It is recommended to manually start installing updates immediately after you install components of Kaspersky Industrial CyberSecurity for Networks. You can configure automatic scheduled start settings for regular installation of updates.

You can use the following update sources:

- Kaspersky update servers.
- Kaspersky Security Center Administration Server.

For an update source, you can also use files from a local resource if installation of updates is started manually.

You can configure the settings and start the installation of updates when connected to the Server through the web interface.

Updates of databases and application modules are subject to the following limitations and special considerations:

- Update functionality is available after a license key is added.

  > Kaspersky software updates including antivirus signatures and the codebase will be unavailable in the United States starting at 12:00 AM Eastern Daylight Time (EDT) on September 10, 2024 in accordance with restrictions.

- After installing the OpenSSL library update, restart the services on the nodes with the installed application components.
- To download updates from Kaspersky update servers, you must have Internet access. When connected to update servers from a computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server, the connection is established over the HTTPS protocol (connection through a proxy server is not supported).
- To download updates from the Kaspersky Security Center Administration Server to Kaspersky Industrial CyberSecurity for Networks, the capability for application interaction with Kaspersky Security Center must be added. You can add this functionality during installation or reinstallation of Kaspersky Industrial CyberSecurity for Networks. Updates are downloaded from the Administration Server repository, which obtains its updates through the corresponding task in Kaspersky Security Center.

Manually starting an update

You can run an update at any time. The capability to run an update is available after a license key is added.

Only users with the Administrator role can manually start an update.

To manually start an update:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.
3. In the **Source for manual update** group of settings, select one of the following options for update sources:
   - Local update source – lets you download updates from files via a specific local path. You can use the **Browse** button to specify the local path to files.
   - **Kaspersky update servers** – for downloading updates from Kaspersky update servers.
   - **Kaspersky Security Center Administration Server** – for downloading updates from the Kaspersky Security Center Administration Server (this option is available if the capability for application interaction with Kaspersky Security Center has been added).
4. Click the **Update now** button.

Configuring automatic updates

After adding a license key, you can configure automatic updates by schedule.

Only users with the Administrator role can configure automatic updates by schedule.

To enable and configure automatic updates by schedule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.
3. Use the **Scheduled update** toggle to enable automatic updates.
4. In the **Source for scheduled update** group of settings, select one of the following options for update sources:
   - **Kaspersky update servers** – for downloading updates from Kaspersky update servers.
   - **Kaspersky Security Center Administration Server** – for downloading updates from the Kaspersky Security Center Administration Server (this option is available if the capability for application interaction with Kaspersky Security Center has been added).
5. Define the update schedule settings. To do so:
   a. In the **Frequency** drop-down list, indicate when the update will occur. Select one of the following options: **Hourly**, **Daily**, **Weekly**, **Monthly**.
   b. Depending on the selected option, specify the values for the settings defining the precise update run schedule.
6. Click the **Save settings** button.

Viewing information about update installation

You can view general and detailed information about update installation.

General information about installed updates

General information provides the dates and times when the updated application modules and databases were released.

To view general information about installed updates:

On the application web interface page, select the **About** section.

Detailed information about update installation

Detailed information contains information about update installation processes that are started. The application saves the following detailed information:

- Date and time when the update process was started
- Update run mode
- Date and time of release of the databases and application modules installed during the update process (if the update was successful)
- Error information (if the update failed)
- List of updated databases and application modules

Detailed information about update installation is saved in the application message log.

Restarting services on the nodes after installing the OpenSSL library update

If the OpenSSL library update is installed on the nodes where the application components are installed, restart the services that ensure the operation of application components on these nodes. The services on the sensor nodes are restarted automatically. If restart of the services on the Server node is required, the application displays notifications about it on the Server web interface page. In this case, to restart the services, you can restart the Server computer or initiate a restart on the web interface page.

Notifications about the need to restart the services on the Server node are displayed in the list of notifications about problems in the application operation, as well as in the **Settings** → **Update** section.

Only the users with the Administrator role can initiate a restart of the Server services on the web interface page.

To restart the services on the Server node using the Server web interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.

3. In the **Restart required** notification, click the **Restart Server** button.

   The service restart process starts. The Application Server is not available for connections until the restart process is complete. During the service restart process, the application web interface page displays a special section named **Application maintenance**.

Distributing access to application functions

In Kaspersky Industrial CyberSecurity for Networks, you can restrict users' access to application functions depending on the tasks of specific users.

The following user accounts may be used to access the application:

- User accounts created in the application.
- Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

It is not possible to connect to the Server under other user accounts or using anonymous connections.

User accounts that have access to the application do not have to be registered as operating system user accounts on the Server computer.

The first application user account must be created during initial configuration of Kaspersky Industrial CyberSecurity for Networks. Then you can create additional user accounts that will be used to perform actions in the application.

Depending on which component you are connected to through the web interface, the following sets of functions are available:

- Application functions when connected to the Server
- Application functions when connected to a sensor

When connected to the Server, the application provides access to functions depending on the role of the user that established the connection.

About application user accounts

Role-based access control (RBAC) is used to restrict access to application functions. The role of an application user account determines the set of actions available to the user. The following roles are provided for application user accounts:

- Administrator.

  A user with the Administrator role has access privileges that enable use of all functions for application management, monitoring, and viewing information. This user can also access functions for managing user accounts created in the application.

- Operator.

  A user with the Operator role has access privileges only for monitoring and viewing information.

The Administrator role is assigned to the first user account that is created during initial configuration of the application.

When adding subsequent user accounts, you can assign the appropriate roles to them. You can create up to 100 user accounts for users of the application (not counting users that are configured for Single Sign-On from Kaspersky Security Center).

When connected to the Server, users receive the access privileges corresponding to the role of their user account. If the role of an application user is changed by another user (who has been assigned the Administrator role) while the user is working, the access rights of the connected user are updated in online mode. For example, a user that has connected to the Server with the Administrator role will lose the rights to access application management functions after the Operator role is assigned to their user account.

You can manage user accounts that were created in the application under **Settings** → **Users** in the Kaspersky Industrial CyberSecurity for Networks web interface.

Application functions that are available when connected to the Server through the web interface

This article presents the application functions that are available to users when connected to the Server through the web interface (see the table below).

Available application functions depending on the user role

Application function	Administrator	Operator
Monitoring the application state when connected through the web interface	✓	✓
Viewing application messages	✓	✓
Enabling and disabling the user activity audit	✓	
Viewing user activity audit entries	✓	
Viewing information about nodes with application components installed and about network interfaces on nodes	✓	✓
Running an application module integrity check when connected to the Server through the web interface	✓	
Managing deployment settings on nodes	✓	
Viewing information about an added license key	✓	✓
Adding a license key	✓	
Removing a license key	✓	
Configuring automatic updates	✓	
Manually starting an update	✓	
Viewing information about update installation	✓	✓
Viewing information about application user accounts	✓	
Creating an application user account	✓	
Changing the role of an application user account	✓	
Deleting an application user account	✓	
Changing a user account password	✓	✓
Viewing the devices table	✓	✓
Viewing address space rules	✓	✓
Viewing address space subnets	✓	✓
Viewing information about devices with IP addresses from the selected subnets	✓	✓
Viewing device information	✓	✓
Selecting sources for device vulnerability monitoring	✓	

Configuring address spaces	✓	
Manually adding devices	✓	
Merging devices	✓	
Deleting devices	✓	
Changing the statuses of devices	✓	
Creating a device group tree	✓	
Automatic grouping of devices based on a specific criterion	✓	
Manually arranging devices into groups	✓	
Adding and removing labels for devices	✓	
Editing device information	✓	
Adding, editing and deleting custom fields for a device	✓	
Configuring Process Control	✓	
Monitoring process parameter values	✓	✓
Viewing Interaction Control rules in the table of allow rules	✓	✓
Manually creating Interaction Control rules	✓	
Editing Interaction Control rule settings	✓	
Enabling and disabling Interaction Control rules	✓	
Deleting Interaction Control rules	✓	
Enabling and disabling sets of Intrusion Detection rules	✓	
Loading and replacing user-defined sets of Intrusion Detection rules	✓	
Removing user-defined sets of Intrusion Detection rules	✓	
Managing the settings for storing log entries in the database	✓	
Managing the settings for saving traffic in the database	✓	
Managing the settings for saving traffic dump files	✓	
Managing the settings for storing risks	✓	
Managing the settings for storing report files	✓	
Changing the logging level for processes	✓	
Configuring operation with EPP applications	✓	
Managing response actions	✓	
Enabling and configuring interaction with Kaspersky Security Center	✓	
Managing connectors	✓	
Adding and deleting connector types	✓	
Performing active polling of devices	✓	
Managing sets of security audit rules	✓	
Managing security audit jobs	✓	
Viewing details on the runs of security audit jobs	✓	✓
Managing account credentials secrets for remote connections	✓	
Configuring event types	✓	
Exporting a security policy to a file	✓	✓
Importing a security policy from a file	✓	
Clearing the current security policy	✓	
System monitoring in online mode	✓	✓

Working with the network interactions map	✓	✓
Moving nodes and groups to other groups on the network interaction map	✓	
Downloading traffic when working with the network interaction map	✓	
Viewing network session details	✓	✓
Downloading network session traffic	✓	
Forming a topology map	✓	
Viewing details about objects on the topology map	✓	✓
Monitoring events and incidents	✓	✓
Managing reports and report templates	✓	
Manually generating reports	✓	✓
Exporting reports to a file	✓	✓
Monitoring risks	✓	✓

Viewing information about application user accounts

When connected to the Server through the web interface, you can view information about user accounts that were created in the application. The application does not display information about Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

Only users with the Administrator role can view information about user accounts.

To view information about application user accounts:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.

   The **Users** tab displays user tiles containing the names and roles of application users.

Creating an application user account

Only users with the Administrator role can create an application user account.

To create an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Add a new user tile. To do so, click the tile with the + icon.

   You will see a new user tile showing fields for entering account credentials and selecting a role for the new user account.
4. In the user name entry field, enter a user name for the account you want to create.

   You can use uppercase and lowercase letters of the English alphabet, numerals, dots, and the _ and - characters.

The user account name must meet the following requirements:

- Must be unique within the list of application user names (not case-sensitive).
- Must contain 3-20 characters.
- Must begin with a letter.
- Must end with any supported character except a dot.

5. In the password entry fields, enter the password that you want to set for the user account.

   The password must meet the following requirements:

   - Must contain between 8 and 256 ASCII characters.
   - Must contain one or more uppercase letters of the English alphabet.
   - Must contain one or more lowercase letters of the Latin alphabet.
   - Must contain one or more numerals.
   - Must contain no more than three consecutive repeated characters.

6. In the drop-down list, select the necessary user role: **Administrator** or **Operator**.
7. Click **Save**.

The user tile displays an icon containing the name of the user account and the role assigned to it.

Changing the role of an application user account

When connected to the Server through the web interface, you can change the roles of user accounts that were created in the application. This role modification method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

Only users with the Administrator role can change the roles of user accounts.

Users with the Administrator role can change the role of any user account except the role of their own user account.

To change the role of an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Click the **Change** button in the user tile of the user whose role you want to change.

   The user tile will switch to account settings editing mode.
4. In the drop-down list, select the necessary user account role: **Administrator** or **Operator**.
5. Click **Save**.

The user tile displays an icon containing the user name and role assigned to this user account.

Deleting an application user account

When connected to the Server through the web interface, you can delete user accounts that were created in the application. This deletion method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

Only users with the Administrator role can delete an application user account.

A user with the Administrator role can delete any user account except their own user account.

To delete an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Users**.

3. Click the **Delete** button in the user tile that you want to delete.

   A window with a confirmation prompt opens.

4. In the prompt window, click **OK**.

Changing a user account password

After connecting to the Server through the web interface, you can change the password of your user account that you used to establish the connection. Only a user account that was created in the application can change a user password on the Kaspersky Industrial CyberSecurity for Networks web interface page. This password change method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

You are advised to change the password in the following cases:

- You are connecting for the first time after the user account was created in the application.

- The current password has been compromised.

- The password must be changed regularly in accordance with the information security requirements at the enterprise.

To change the password of your own user account:

1. On the Kaspersky Industrial CyberSecurity for Networks web interface page, open the user menu:

   - If the menu is collapsed, click the 👤 button.

   - If the menu is expanded, click the button on the right of the name of the current user.

2. In the user menu, select **Change password**.

   The **Change password** window appears.

3. In the **Current password** field, enter your current password.

4. In the **New password** and **Repeat new password** fields, enter the new password.

   The new password must meet the conditions listed in the **Change password** window. The conditions you fulfill are automatically marked while you are entering your password.

5. Click the **Edit** button. This button is available after entering the current password and new password and after fulfilling all requirements for the new password.

The new password will be required the next time you connect to the Server through the web interface.

Configuring Asset Management

Kaspersky Industrial CyberSecurity for Networks lets you monitor the assets of a company as represented by its industrial network devices. Devices are identified by the application based on their MAC- and/or IP addresses. The application can receive device data when doing the following:

- Processing traffic arriving through monitoring points

- Processing data received from EPP applications

A devices table is created for the purpose of asset management in the application. The table is populated based on the address spaces configured in the application.

The application can automatically obtain information about devices. Only information that can be identified by the application may be automatically obtained and updated (for example, address information of a device).

For device activity detection and automatic update of information, the corresponding Asset Management methods must be enabled. If necessary, you can manually specify the values of specific data and disable their automatic update to lock the current values (for example, you can lock the device category if the currently defined category differs from the one that is determined automatically).

Some device information must be specified manually because it cannot be automatically updated. For example, you can save specific device information in the device table, and add any absent criteria for sorting and filtering devices. You can also use manually defined information to arrange devices in various groups in the group tree, or filter and search for devices based on device labels.

You can configure Asset Control and edit device information in the **Assets** section of the **Devices** tab. You can also view information about the interactions between devices and perform various actions with devices when working with the network interactions map and with the topology map. To conveniently present information about interactions between devices and to enable automatic grouping of devices by subnet, you can generate lists of subnets in the address space based on the specific IP addressing of devices in your company's network.

Asset Management methods and modes

The following methods are used for asset management in Kaspersky Industrial CyberSecurity for Networks:

- Device activity detection This method lets you monitor the activity of devices in industrial network traffic based on the obtained MAC- and/or IP addresses of devices.

- Device Information Detection This method lets you automatically obtain and update device information based on data received from traffic or from EPP applications.

- PLC Project Control This method lets you detect information about PLC projects in traffic, save this information in the application, and compare it to previously obtained information.
- Risk Detection. This method lets you detect information security risks based on information about devices and their interactions.
- Network Session Detection. This method analyzes industrial network traffic to detect network sessions created by devices for the purpose of connecting to other devices.

You can enable and disable the use of individual asset management methods.

About the device activity detection method

The following modes are available for the device activity detection method:

- Learning mode. This mode is intended for temporary use. In this mode, all devices whose activity is detected in traffic are considered to be authorized by the application. You can enable learning mode only for the device activity detection method. The device activity detection method can be applied together with other asset management methods.
- Monitoring mode. This mode is intended for continual use. In this mode, when activity of devices is detected, the application considers only those devices that have been assigned the *Authorized* status as authorized.

Depending on the selected mode, the application automatically assigns statuses to devices.

In learning mode, the application does not register events when it detects activity of devices or when device information is automatically updated.

You can configure the learning mode for the device activity detection method. Asset management learning mode must be enabled for a sufficient amount of time to detect the activity of relevant devices. This amount of time depends on the number of devices in the industrial network and how frequently they operate and are serviced. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period from one to several days to detect the activity of all required devices.

The received MAC- and IP addresses of devices are processed with the following special considerations:

- A router indicator must be set for devices that perform functions of a network switch between industrial network segments. If this indicator is not defined automatically by the application, it must be set manually. Otherwise, the application may fail to populate the devices table with devices that interact through this routing device in different industrial network segments. After the indicator is set, interacting devices will be added to the devices table when there is corresponding traffic involving them.
- If only the device IP address is detected in traffic (the IP address cannot be matched to a specific MAC address), this IP address is checked against the list of subnets known to the application. For the device activity detection method, IP addresses that belong only to **Public** subnets are not taken into account.

About the device information detection method

When the device information detection method is enabled, the application automatically updates information about devices. For example, the application can update the name of the operating system installed on a device as it detects updated data in the traffic of the device.

By default, automatic update is enabled for all information. For some types of information, in the device settings, you can disable automatic update in the following cases: adding a device manually, merging devices, and changing the device information.

To automatically get information about devices, the application can use:

- Built-in *rules for detection of information about devices and device communication protocols*.

  After installation, the application uses the default rules for identifying information about devices and the protocols of communication between devices. To increase the accuracy of identifying information, Kaspersky experts regularly update the databases containing the sets of rules. You can update rules by installing updates.

- Data from EPP applications containing information about the devices.

  The application processes data from EPP applications, which contain information about devices (for example, equipment information).

- Data from EPP applications processed according to the rules from the *Kaspersky ICS CERT vulnerabilities database for SCADA*.

  Rules from the Kaspersky ICS CERT vulnerabilities database for SCADA provide for additional analysis of data received from EPP applications. Based on the analysis results, the application can indirectly determine some information about the devices (for example, the device category). The **Kaspersky ICS CERT vulnerabilities database for SCADA** is a system-based set of security audit rules. These rule set is supplied and updated together with the database and application module updates. Therefore, to use the rules from this set, install the updates.

About events registered when applying methods

In monitoring mode, the application registers the corresponding events based on Asset Management technology. Depending on the applied methods, events may be registered in the following cases:

- Detection of activity of unknown devices or devices with the *Archived* status.
- Automatic change of device information.
- Detection of read/write operations with projects and PLC project blocks.
- Detection of Vulnerability risks and changes related to these risks.

When PLC Project Control is enabled, the application may register a large number of events associated with the detection of read/write operations with projects or blocks. Normally, a large number of events are registered at the initial stage when this method is used. To reduce the total number of registered events, the PLC Project Control method is disabled by default after the application is installed. You can enable this method at any time.

Selecting sources of vulnerability data

When monitoring risks, the application detects vulnerabilities of devices by using information from the database of known vulnerabilities. Kaspersky experts upload vulnerability information to the database from various data sources.

By default, the application detects vulnerabilities of devices based on the information that has been uploaded to the database from all sources. If necessary, you can select relevant sources to detect vulnerabilities of devices based on the information from only these sources.

Only users with the Administrator role can select sources for device vulnerability detection.

To enable or disable use of sources for vulnerability detection:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. In the **Risks** section, click the **Sources of vulnerabilities** button to open the window for selecting sources.

3. Enable or disable the use of specific sources. The list contains all sources in the database of known vulnerabilities.

4. Click the **Apply** button.

Manually adding devices

You can manually add a new device to the devices table. For an added device, you must specify its MAC address and/or IP address.

> The MAC- and IP addresses of an added device must be unique within the address space containing these addresses. If additional address spaces were added to the application, you can add devices with identical addresses to different address spaces.

Only users with the Administrator role can manually add devices.

You can add devices in the following ways:

- **Adding a device when working with the devices table** ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. On the **Devices** tab in the **Assets** section, open the details area by clicking the **Add device** button.

3. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.

4. On the **Address information** tab in the details area, specify the MAC- and/or IP addresses of the device.

5. If additional address spaces were added to the application, specify the names of the address spaces for addresses.

6. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:

   - If you want to add an IP address, click the **Add IP address** button.

   - If you want to remove an IP address, click the 🗑 icon located on the right of the field containing the IP address.

7. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To do so, perform one of the following actions:

   - If you want to add a network interface, click the **Add interface** button located under the group of settings of the last network interface of the device.

   - If you want to delete a network interface, click the ✕ icon displayed to the right of the device network interface name (if there are two or more network interfaces).

   - If you want to define a different name for a network interface, click the ✎ icon located on the right of the current name and enter the new name for the network interface in the field that opens.

8. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the 🔒 and 🔓 icons. On the **Settings** tab, the 🔒 and 🔓 icons are located on the left side of the fields. On the **Address information** tab, the 🔒 and 🔓 icons are located to the right of the network interface name.

9. On the **Custom fields** tab in the details area, create a list of custom fields if necessary.

10. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

The devices table will show the new device with the *Authorized* status.

- Adding a device when working with the topology map

When working with the topology map, you can add a new device to the devices table.

To add a new device to the device table when working with a topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, in the **Add node** drop-down list, select **New device**.

   A details area with the device settings appears in the right part of the window.
3. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.
4. On the **Address information** tab in the details area, specify the MAC- and/or IP addresses of the device.
5. If additional address spaces were added to the application, specify the names of the address spaces for addresses.
6. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:
   - If you want to add an IP address, click the **Add IP address** button.
   - If you want to remove an IP address, click the 🗑 icon located on the right of the field containing the IP address.
7. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To do so, perform one of the following actions:
   - If you want to add a network interface, click the **Add interface** button located under the group of settings of the last network interface of the device.
   - If you want to delete a network interface, click the × icon displayed to the right of the device network interface name (if there are two or more network interfaces).
   - If you want to define a different name for a network interface, click the ✎ icon located on the right of the current name and enter the new name for the network interface in the field that opens.
8. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the 🔒 and 🔓 icons. On the **Settings** tab, the 🔒 and 🔓 icons are located on the left side of the fields. On the **Address information** tab, the 🔒 and 🔓 icons are located to the right of the network interface name.
9. On the **Custom fields** tab in the details area, create a list of custom fields if necessary.
10. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

The devices table will show the new device with the *Authorized* status.

- Adding a device based on the node of an unknown device on the network interactions map ?

When working with the network interactions map, you can add a new device to the devices table using a node representing a device that is unknown to the application.

To add a node of an unknown device to the devices table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interaction map** tab in the **Network map** section, select the necessary node representing a device unknown to the application.

   The details area appears in the right part of the web interface window.
3. Click the **Add to the devices table** button.

   The details area will show the tabs for configuring the settings of the new device.
4. Configure the settings of the new device without changing the MAC- and/or IP address that are specified for the node.

   For a description of how to configure these settings, please refer to the procedure for manually adding a device when working with the devices table.
5. Click **Save**.

The devices table will show the new device with the *Authorized* status. The node that previously represented a device that was unknown to the application will now represent a device on the network interactions map.

- Adding a device based on an unmanaged switch on the topology map ?

When working with the topology map, you can add a new device to the devices table using a node representing an unmanaged switch.

To add a node of an unmanaged switch to the devices table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, select the relevant node that represents the unmanaged switch.

   The details area appears in the right part of the web interface window.
3. Click the **Add to the devices table** button.

   The details area will show the tabs for configuring the settings of the new device.
4. Specify the MAC address and/or IP address of the device and configure all other settings.

   For a description of how to configure these settings, please refer to the procedure for manually adding a device when working with the devices table.
5. Click **Save**.

The devices table will show the new device with the *Authorized* status. The node that previously represented the unmanaged switch will now represent a known device on the topology map.

After adding a device, you can add Process Control settings for the device.

Merging devices

If one device is represented by multiple devices in the table for some reason, these devices can be merged into one device. Devices can be merged automatically when the device activity detection method is enabled in learning mode. You can also manually merge devices.

Devices are automatically merged if the application identifies a connection between the MAC address of one device and the IP address of a different device, or identifies a connection between devices according to the results of an active poll or data received from EPP applications. If conflicts arise between defined values in device information, the merged device will retain the values that were defined for the following devices:

- Devices with IP addresses, if a connection is detected between the MAC address of one device and the IP address of a different device.

  > Prior to enabling learning mode (and while working in this mode), it is not recommended to change information about devices for which only a MAC address is defined if they could be automatically merged with devices that have defined IP addresses.

- Devices with IP addresses and Kaspersky Endpoint Agent installed, if a connection is detected between devices according to data from EPP applications.
- Devices with the most IP addresses.
- Devices with the most addresses, if the devices do not have an IP address.

When devices are merged, some information from the merged devices might not be saved in the new device (for example, the contents of dynamic fields and topology parameters). In addition, to merge devices, the total number of network interfaces in the new device must not be more than 512.

Only a user with the Administrator role can manually merge devices.

You can merge devices in the following ways:

- **Merging devices when working with the devices table**

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices that you want to merge.

4. Click the **Merge devices** button.

   The details area with the tabs for configuring the new device settings appears in the right part of the window.

5. Check the settings of the new device and edit them if necessary:

   - On the **Settings** tab in the details area, all fields containing conflicting values in the selected devices are marked by messages regarding the conflicting values. The conflicting values are merged into one value in text fields. If necessary, enable or disable automatic updates for the relevant information about the device.

   - On the **Address information** tab, in the details area, the MAC and IP addresses of the selected devices are distributed by individual network interfaces. If necessary, change the values of addresses, address spaces, and the names of network interfaces, and enable or disable automatic updates for the relevant information about the device.

   - On the **Custom fields** tab in the details area, the list contains all custom fields of the selected devices.

6. Click the **Merge** button.

   A window with a confirmation prompt opens.

7. In the prompt window, click **OK**.

The devices table will show the new device with the *Authorized* status.

- **Merging devices when working with the networking interactions map and the topology map**

When working with the network interactions map, and the topology map, you can merge multiple nodes on the maps into one new device for the devices table.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

WAN nodes cannot be merged.

To merge devices represented by nodes on the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select several objects which represent nodes and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.

   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.

4. Click the **Merge devices** button.

   The details area with the tabs for configuring the new device settings appears in the right part of the window.

5. Check the settings of the new device and edit them if necessary:

   - On the **Settings** tab in the details area, all fields containing conflicting values in the selected devices are marked by messages regarding the conflicting values. The conflicting values are merged into one value in text fields. If necessary, enable or disable automatic updates for the relevant information about the device.

   - On the **Address information** tab, in the details area, the MAC and IP addresses of the selected devices are distributed by individual network interfaces. If necessary, change the values of addresses, address spaces, and the names of network interfaces, and enable or disable automatic updates for the relevant information about the device.

   - On the **Custom fields** tab in the details area, the list contains all custom fields of the selected devices.

6. Click the **Merge** button.

   A window with a confirmation prompt opens.

7. In the prompt window, click **OK**.

The devices table will show the new device with the *Authorized* status. The network map will show one merged node instead of the previously selected multiple nodes.

Deleting devices

You can delete one or multiple devices from the devices table.

Only a user with the Administrator role can delete devices.

Information about deleted devices is not saved in the application. If deleted devices start displaying activity in the industrial network again, the application will add them to the devices table as new devices (with the *Authorized* or *Unauthorized* status depending on the current asset management mode).

You can delete devices in the following ways:

- Deleting devices when working with the devices table ?

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
  2. Select the **Assets** section.
  3. On the **Devices** tab, select the devices that you want to delete.
  4. Right-click to open the context menu of one of the selected devices.
  5. In the context menu, select one of the following options:
     - **Delete device** if one device is selected.
     - **Delete devices** if multiple devices are selected.

     A window with a confirmation prompt opens.
  6. In the prompt window, click **OK**.

- Removing devices when working with the networking interactions map and the topology map ?

When working with the network interactions map and the topology map, you can remove devices from the devices table by using the nodes representing those devices on the maps.

To remove a device when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select the node representing the device you want to remove.

   The details area appears in the right part of the web interface window.

4. Click the **Delete** button.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Manually changing the statuses of devices

Only a user with the Administrator role can change the statuses of devices.

You can change the status (select either the *Authorized*, *Unauthorized* or *Archived* status) for one selected device or for multiple selected devices simultaneously. If you are changing the status of one selected device, you can enable or disable the automatic status change of that device to the *Archived* status.

The application automatically changes the status of an *Archived* device if it displays activity. Depending on the current asset management mode, the application assigns either the *Authorized* or *Unauthorized* status to the detected device.

You can change the statuses of devices in the following ways:

- **Changing the statuses of devices when working with the devices table**

To change the status of one device when working with the devices table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Devices** tab in the **Assets** section, select the relevant device.

   The details area appears in the right part of the web interface window.
3. Click the **Edit** button.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.
4. Select the **Settings** tab.
5. In the **Status** drop-down list, select the necessary status of the device.
6. Enable or disable the automatic status changes of devices to the *Archived* status. To do this, use the icon located in the **Status** drop-down list.

   You may need to disable automatic status changes if, for example, you want to prevent the *Authorized* status from changing to the *Archived* status for a rarely connected device.
7. Click **Save**.

To change the status of multiple devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Devices** section.
3. In the devices table, select the devices whose status you want to change.
4. Open the **Change status** drop-down list in the toolbar.
5. In the drop-down list, select the command to assign the required status.

   A window with a confirmation prompt opens.
6. In the prompt window, click **OK**.

- Changing the statuses of devices when working with the networking interactions map and the topology map

When working with the network interactions map and the topology map, you can change the statuses of known devices represented by nodes on the maps.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To change the status of one device when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select the node of the relevant device.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.

5. Select the **Settings** tab.

6. In the **Status** drop-down list, select the necessary status of the device.

7. Enable or disable the automatic status changes of devices to the *Archived* status. To do this, use the icon in the **Status** drop-down list.

   You may need to disable automatic status changes if, for example, you want to prevent the *Authorized* status from changing to the *Archived* status for a rarely connected device.

8. Click **Save**.

To change the status of multiple devices when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select the objects which represent nodes of known applications and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the `SHIFT` key and use your mouse to select a rectangular area containing the relevant objects.

   - Hold down the `CTRL` key and use your mouse to select the relevant objects.

4. Open the **Change status** drop-down list in the toolbar.

5. In the drop-down list, select the command to assign the required status.

   A window with a confirmation prompt opens.

6. In the prompt window, click **OK**.

About arranging devices into groups

You can use the device group tree to arrange devices into groups. The device group tree supports up to six nesting levels.

Devices can be put into groups at any level of the hierarchy. However, each device can be added to only one of the groups in the tree.

The tree also has a limit of no more than 1,000 groups.

Until a device is added to a specific group, information about this device does not contain any information about the specific location of the device. This device is assigned to the top level of the hierarchy within the group tree. After a device is added to a group, the application saves the location of this device as the full path to the group in the group tree.

Devices can be arranged into groups in the following ways:

- Automatically group devices based on a specific criterion.

  Using this type of device grouping, the application can automatically add groups to the device group tree. Groups are added when the application detects devices whose information matches the selected grouping criterion. The names of groups are assigned from a range of specific values for the selected criterion (for example, from the names of device categories when grouping by category).

- Manually arrange devices into groups.

  You can manually arrange devices into groups, including by adding devices into relevant groups and excluding them from other groups. When necessary, you can make changes to the device group tree by utilizing the available functions for manually forming the device group tree.

Automatic grouping of devices based on a specific criterion

You can automatically group devices in the device group tree based on one of the following criteria:

- Affiliation of IP addresses with subnets that are known to the application
- Device categories
- Device vendors

Only users with the Administrator role can automatically group devices.

You can automatically group devices in the following ways:

- **Automatically grouping devices based on a specific criterion beginning with the top level of the hierarchy in the group tree** ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. On the **Network interactions map** tab in the **Network map** section, click one of the following buttons for selecting a grouping criterion in the toolbar located in the left part of the network interactions map display area:

   - – for grouping devices by subnet.

   - – for grouping devices by category.

   - – for grouping devices by vendor.

   A window opens with a prompt for you to select a grouping option.

3. If you need to group devices by category and vendor based on address spaces, in the prompt window select the **Take into account the address spaces** check box.

4. Click one of the following buttons depending on your desired result:

   - If you want to group devices by subnets, click the **Group** button.

   - If you want to group devices by category and vendor based on address spaces in all groups of the device group tree, click the **With child groups** button.

   - If you want to group devices by category and vendor based on address spaces only at the top level of the device group tree hierarchy, click the **Selected only** button.

The application will identify the devices that match the selected grouping criterion, create groups for these devices, and place the devices into these groups.

- Automatically grouping devices in a selected device group:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, select the group in which you want to automatically group devices.
3. Right-click to open the context menu.
4. In the context menu, select one of the following options:
   - **Group by subnet**.
   - **Group by category**.
   - **Group by vendor**.

   A window opens with a prompt for you to select a grouping option.
5. If you need to group devices by category and vendor based on address spaces, in the prompt window select the **Take into account the address spaces** check box.
6. In the prompt window, click one of the following buttons depending on your desired result:
   - If you want to group devices by subnets, click the **Group** button.
   - If you want to group devices by category or vendor in all child groups of the selected group, click the **With child groups** button.
   - If you want to group devices by category or vendor only in the selected group, click the **Selected only** button.

The application will identify the devices that match the selected grouping criterion, create groups for these devices, and place the devices into these groups (however, devices that are already in other groups will not be put into the new groups).

Manually arranging devices into groups

Only users with the Administrator role can manage the location of devices within the group tree.

To manage the arrangement of devices in the group tree, you can use the following functions:

- Add one device to a group ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device to add to a group on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. Click the **Edit** button.

4. In the details area, go to the **Settings** tab.

5. Click the ▙ icon in the right part of the **Group** field.

   The **Select group in tree** window appears.

6. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.

7. Click the **Select** button.

   The path to the selected group will appear in the **Group** field.

8. Click **Save** in the details area.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

- Add multiple devices to a group

You can add multiple devices to a group when working with the devices table.

When working with the network interactions map, you can also add multiple known devices represented by nodes on the map to a group. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To add multiple devices to a group when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Devices** tab, select the devices that you want to add to a group.
4. Right-click to open the context menu.
5. In the context menu, select the **Move to group** option.

   The **Select group in tree** window appears.
6. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.
7. Click the **Select** button.

   The path to the selected group will appear in the **Group** field.

To add multiple devices to a group when working with the network interactions map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, select the relevant nodes of known devices and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.
3. Right-click to open the context menu.
4. In the context menu, select the **Move to group** option.

   The **Select group in tree** window appears.
5. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.
6. Click the **Select** button.

   The selected nodes representing known devices will be displayed within the selected group.

- Remove one device from a group ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device to remove from a group on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.
3. Click the **Edit** button.
4. In the details area, go to the **Settings** tab.
5. In the **Group** field, delete the path to the group by clicking the × icon in the field (the icon is displayed if a group is defined).
6. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

After saving the changes for the device, the **Group** parameter is cleared and the device will be assigned to the top level of the hierarchy within the group tree.

- Remove multiple devices from groups ?

You can remove multiple devices from groups when working with the devices table. The devices selected for removal from groups may be part of the same group or in different groups.

When working with the network interactions map, you can also remove multiple known devices represented by nodes on the map from groups. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To remove multiple devices from groups when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Devices** tab, select the devices that you want to remove from groups.
4. Right-click to open the context menu.
5. In the context menu, select the **Remove from group** option.

   A window with a confirmation prompt opens.
6. In the prompt window, confirm removal of the devices from groups.

For all selected devices, the **Group** parameter is cleared and these devices will be assigned to the top level of the hierarchy within the group tree.

To remove multiple devices from groups when working with the network interactions map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, select the nodes in expanded groups and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.
3. Right-click to open the context menu.
4. In the context menu, select the **Remove from group** option.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm removal of the devices from groups.

For all selected devices, the **Group** parameter is cleared and these devices will be displayed outside of groups.

Moving nodes and groups to other groups on the network interaction map

You can change the location of nodes and groups in the device group tree by dragging objects on the network interactions map. After being moved, nodes and groups change their location in the device group tree just as when adding devices to a group and removing devices from groups.

Only users with the Administrator role can move nodes and groups to other groups.

To move nodes and/or groups to other groups:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, select the relevant nodes of known devices and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.
3. Move the cursor over one of the selected objects (group or node representing a known device).
4. Press the **CTRL** key and hold it down while dragging the selected objects to the relevant group (or to any place outside of groups if you want to move the selected objects to the top level of the hierarchy within the group tree).

   A window with a confirmation prompt opens.
5. In the prompt window, confirm movement of the selected objects.

Manually creating a device group tree

You can create a device group tree when working with the devices table, with the network interactions map and the topology map. Tree creation functions are available in the **Create group tree** or **Select group in tree** window.

Only users with the Administrator role can create a device group tree.

To utilize the functions for creating a device group tree:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. In the **Assets** section on the **Devices** tab or in the **Network map** section, do one of the following:

   - Open the **Create group tree** window by clicking the **Configure groups** button.

     The **Configure groups** button in the **Assets** section is available in the **Group management** drop-down list in the toolbar.

     The **Configure groups** button in the **Network map** section is only available on the **Network interactions map** tab.

- Open the **Select group in tree** window by adding devices to groups. You can also open this window when filtering the devices table by the **Group** column.

Any changes made to the device group tree in the **Create group tree** or **Select group in tree** window are applied immediately.

To create the device group tree, you can use the following functions:

- Add group ?

  1. In the **Create group tree** or **Select group in tree** window, add a new group in one of the following ways:
     - If the tree is empty and you want to add the first group, click the **Add** button or press either the `INSERT` or `ENTER` key.
     - If you want to add a group on the same hierarchical level as an existing group, select this group and press `ENTER`.
     - If you want to add a child group to an existing group, select this group and click the **Add** button or press the `INSERT` key.
  2. In the entry field, enter the group name.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

     The group name must meet the following requirements:
     - Must begin and end with any permitted character except a space.
     - Must contain 255 characters or less.
     - Must not match the name of any other group included under the same parent group (not case-sensitive).
  3. Click the ✓ icon on the right of the entry field.

- Rename group ?

1. In the **Create group tree** or **Select group in tree** window, select the group that you want to rename.
2. Click the **Rename** button or press **F2**.
3. In the entry field, enter the new name of the group.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   The group name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of any other group included under the same parent group (not case-sensitive).
4. Click the ✓ icon on the right of the entry field.

The new group name will appear in the information about devices that are added to this group or to its child groups.

- Deleting groups ?

When a group is deleted, the devices that were added to that group are not deleted. Instead, the devices from the deleted group are moved to the same level in the device tree hierarchy where the deleted group had been.

To delete a group from the device group tree:

1. In the **Create group tree** or **Select group in tree** window, select the group that you want to delete.
2. Click the 🗑 icon.

   This opens a window prompting you to select a deletion option.
3. In the prompt window, click one of the following buttons depending on your desired result:

   - If you want to delete only the selected group and leave its child groups, click the **Selected only** button.
   - If you want to delete the selected group together with all of its child groups, click the **With child groups** button.

   A window with a confirmation prompt opens.
4. In the prompt window, click **OK**.

- Move group ?

1. In the **Create group tree** or **Select group in tree** window, select the group that you want to move.
2. Use the arrow icons or their corresponding key combinations **ALT+↓**, **ALT+↑**, **ALT+←**, or **ALT+→** to move the group relative to other elements of the tree. If an operation cannot be performed, the icon for the operation is not available.

- Search groups

  You can find relevant groups in the device group tree by using the **Search groups** field in the **Create group tree** or **Select group in tree** window. Groups that meet the search criteria are displayed in the device group tree. For groups that are child groups, their parent groups are also displayed.

- Update the tree

  The composition of groups in the device group tree could be changed on the Server while you are working with the tree (for example, it could be changed by another user who is connected to the Server).

  You can manually update the tree by using the ↻ icon in the **Create group tree** or **Select group in tree** window.

Adding and removing labels for devices

You can assign any user-defined labels to devices.

A *device label* contains a text description that helps you quickly find or filter devices in the table. Any convenient text descriptions can be saved as labels. You can assign up to 16 labels for a device. Each device can have its own set of labels.

Lists of device labels are displayed in the devices table in the **Labels** column. Labels in a cell are sorted in alphabetical order.

Only users with the Administrator role can add or remove labels for devices.

Labels can be added or removed in the following ways:

- Adding labels for one device

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select a device for adding a label on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. Click the **Edit** button.

   In the details area, go to the **Settings** tab.

4. In the **Labels** field, enter the text descriptions that you want to use as labels. To separate labels, you can use the `ENTER` key or the `;` character.

   You can use uppercase and lowercase letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A label name must meet the following requirements:

   - Must begin and end with any permitted character except a space.

   - Unique in the list of device labels (not case-sensitive).

   - Contains from 1 to 255 characters.

5. If necessary, use the **Copy labels** link to copy the list of labels. The link is displayed if the list of labels is not empty.

6. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

- Adding labels for multiple devices

You can add labels for multiple devices when working with the devices table.

When working with the network interactions map and the topology map, you can add labels for known devices represented by nodes on the maps. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To add labels for multiple devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to add labels.

4. Right-click to open the context menu of one of the selected devices.

5. In context menu select **Add labels**.

   The **Add labels** window opens.

6. In the **Labels** field, enter the text descriptions that you want to use as labels. To separate labels, you can use the `ENTER` key or the `;` character.

   You can use uppercase and lowercase letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A label name must meet the following requirements:

   - Must begin and end with any permitted character except a space.

   - Unique in the list of device labels (not case-sensitive).

   - Contains from 1 to 255 characters.

7. If necessary, use the **Copy labels** link to copy the list of labels. The link is displayed if the list of labels is not empty.

8. If you want to clear the current lists of labels for selected devices and provide only new labels for these devices, select the **Delete existing** check box.

   > If the **Delete existing** check box is cleared, the current list of labels will remain on each device. The new labels will be added to the lists of labels on all selected devices. In this case, the total number of labels for some of the selected devices may exceed the limit (up to 16 labels for each device). The application checks this limit before adding new labels.

9. Click **OK**.

   The button is not available if the names of entered labels do not meet the requirements, or if the list of labels is empty while the **Delete existing** check box is cleared.

To add labels for multiple devices when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select the relevant nodes of known applications and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.

   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.

4. Right-click to open the context menu of one of the selected objects.

5. In context menu select **Add labels**.

   The **Add labels** window opens.

6. In the **Labels** field, enter the text descriptions that you want to use as labels. To separate labels, you can use the **`ENTER`** key or the `;` character.

   You can use uppercase and lowercase letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A label name must meet the following requirements:

   - Must begin and end with any permitted character except a space.

   - Unique in the list of device labels (not case-sensitive).

   - Contains from 1 to 255 characters.

7. If necessary, use the **Copy labels** link to copy the list of labels. The link is displayed if the list of labels is not empty.

8. If you want to clear the current lists of labels for selected devices and provide only new labels for these devices, select the **Delete existing** check box.

   > If the **Delete existing** check box is cleared, the current list of labels will remain on each device. The new labels will be added to the lists of labels on all selected devices. In this case, the total number of labels for some of the selected devices may exceed the limit (up to 16 labels for each device). The application checks this limit before adding new labels.

9. Click **OK**.

   The button is not available if the names of entered labels do not meet the requirements, or if the list of labels is empty while the **Delete existing** check box is cleared.

- Removing labels from one device

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select a device for removing a label on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. Click the **Edit** button.

   In the details area, go to the **Settings** tab.

4. In the **Labels** field, delete the unnecessary labels:

   - If you want to delete specific labels, use the × icon next to the names of the labels.
   - If you want to delete all labels, use the × icon on the right side of the **Labels** field.

5. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

- Clearing lists of labels for multiple devices ?

You can clear the lists of labels for multiple devices when working with the devices table.

When working with the network interactions map and the topology map, you can clear the lists of labels for known devices represented by nodes on the maps. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To clear the lists of labels for multiple devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Devices** tab, select the devices for which you want to clear the lists of labels.
4. Right-click to open the context menu of one of the selected devices.
5. In context menu select **Add labels**.

   The **Add labels** window opens.
6. Select the **Delete existing** check box.
7. Click **OK**.

To clear the lists of labels for multiple devices when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Network map** section.
3. On the **Network interactions map** or **Topology map** tab, select the relevant nodes of known applications and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.
4. Right-click to open the context menu of one of the selected objects.
5. In context menu select **Add labels**.

   The **Add labels** window opens.
6. Select the **Delete existing** check box.
7. Click **OK**.

Editing device information

Only users with the Administrator role can change device information.

To manually edit device information:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Devices** tab in the **Assets** section, select the relevant device.

   The details area appears in the right part of the web interface window.
3. Click the **Edit** button.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.
4. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.
5. On the **Address information** tab in the details area, specify the MAC- and/or IP addresses of the device.
6. If additional address spaces were added to the application, specify the names of the address spaces for addresses.
7. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:
   - If you want to add an IP address, click the **Add IP address** button.
   - If you want to remove an IP address, click the 🗑 icon located on the right of the field containing the IP address.
8. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To generate a list of network interfaces of a device, perform one of the following actions:
   - If you want to add a network interface, click the **Add interface** button located under the group of settings of the last network interface of the device.
   - If you want to delete a network interface, click the × icon displayed to the right of the device network interface name (if there are two or more network interfaces).
   - If you want to define a different name for a network interface, click the ✎ icon located on the right of the current name and enter the new name for the network interface in the field that opens.
9. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the 🔒 and 🔓 icons. On the **Settings** tab, the 🔒 and 🔓 icons are located on the left side of the fields. On the **Address information** tab, the 🔒 and 🔓 icons are located to the right of the network interface name. For the **Status** field, automatic changes in device statuses can be enabled or disabled by using the ▣ icon.
10. On the **Custom fields** tab in the details area, create a list of custom fields and their values if necessary.
11. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

After saving changes to device information, you can add or edit the Process Control settings for a device.

Adding, editing and deleting custom fields for a device

You can add, edit and delete custom fields containing information about devices. Custom fields are displayed in the details area when a device is selected.

For custom fields, the following limitations apply:

- The number of custom fields for one device shall not exceed 16.
- The number of characters in the field name can be no more than 100.
- The number of characters in the field value can be no more than 1,024.

Only users with the Administrator role can add, edit, or delete custom fields.

To add, edit, or delete a custom field:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Devices** tab in the **Assets** section, select the relevant device.

   The details area appears in the right part of the web interface window.
3. Click the **Edit** button.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.
4. Go to the **Custom fields** tab and perform one of the following actions:
   - If you want to add a custom field, click the **Add custom field** button and in the opened fields enter the name and value for the custom field.
   - If you want to edit a custom field, enter the new name and/or value of the relevant custom field.
   - If you want to delete a custom field, click the × icon located on the right of the custom field name.
5. Click **Save**.

Configuring address spaces

Kaspersky Industrial CyberSecurity for Networks monitors devices and their interactions while accounting for their address spaces (hereinafter also referred to as "AS"). *Address spaces* are intended for arranging addresses of devices into sets based on a specific attribute (for example, based on the specific network segments of devices).

Lists of rules and subnets are used to describe address spaces in the application.

An *address space rule* is a set of parameters that define the conditions for including addresses into a specific address space. To bind an address to an address space, each MAC or IP address must satisfy at least one address space rule. The application binds an address to the address space whose rule defines the most specific conditions for affiliation of this address (for example, if the address is explicitly specified in the rule).

Address space subnets are used to verify IP addresses detected by the application. Depending on the type of subnet that a detected IP address belongs to, the application may take different actions for asset management and device interaction control.

You can configure address spaces in the **Assets** section of the **Address spaces** tab. Each address space is presented as a data block containing information about the address space. This data block consists of a header and nested blocks containing tables of rules and subnets. When viewing information about address spaces, you can expand and collapse the contents of data blocks.

Default address space

By default, one shared address space named **Default** is defined in the application. This address space contains a single rule whose settings are configured to bind any MAC- and IP address to this specific address space. By default, the list of subnets of the **Default** address space contains a standard set of subnets that are most frequently used at organizations.

You cannot edit the rule of the **Default** address space or add other rules to this address space. However, users with the Administrator role can edit the list of subnets in this address space to generate a set of subnets while taking into account the specific IP addressing of devices within the network of your organization. If Kaspersky Industrial CyberSecurity for Networks receives data from EPP applications, the application can use this data to automatically add subnets to the list of subnets.

Additional address spaces

If necessary, you can configure multiple address spaces in addition to the **Default** address space. You can generate user-defined rules and sets of subnets for added address spaces. Addresses that satisfy the conditions of the added address spaces will be bound to these address spaces. All other addresses will remain bound to the **Default** address space.

You may need to add address spaces when using devices that have identical addresses in different network segments, for example. In this case, after adding and configuring address spaces, the application will be able to distinguish address information based on additional attributes that the application will add to addresses in the form of address space names.

For examples of using address spaces, see the Appendices.

Binding addresses to address spaces

When using multiple address spaces, the application adds attributes containing the names of address spaces to all addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. Attributes containing the names of address spaces are no longer displayed for addresses if all added address spaces are deleted from the application (attributes of address spaces remain only for addresses in events and in certain risks associated with devices).

Attributes containing the names of address spaces denote the links between addresses and address spaces. Addresses that are bound to address spaces become dependent on these address spaces.

> When deleting an address space that is bound to addresses, the application automatically deletes all addresses that are bound to the address space being deleted. These addresses are deleted from all application objects except events. When deleting an address from an object, the application checks for any other remaining addresses in this object. If there are no other remaining addresses, the application also deletes the object (such as a device).

About address space rules

The rules of address spaces are displayed in the **Rules** blocks within descriptions of address spaces. Information about rules is displayed in the address space header and in the rules table.

The settings of address space rules are displayed in the following columns of the table:

- **Data source**.

  Type of source of incoming address information and list of selected data sources. The following types of data sources are available:

  - **Monitoring points** – selected for a monitoring point rule.
  - **Integration servers** – selected for an integration servers rule (the data on address information received from the selected integration servers will satisfy the address space rule).
  - **Active polling modules** – selected for an active polling modules connectors rule. (the data on address information received from the selected active polling modules will satisfy the address space rule).

- **OSI model layers**.

  Selected layers of the Open Systems Interconnection (OSI) model for an address space rule. A rule can be configured for addresses of the following OSI layers:

  - **Data Link (L2)** – MAC addresses.
  - **Network (L3)** – IP addresses.
  - **Data Link and Network (L2 and L3)** – MAC addresses and IP addresses.

- **VLAN ID**.

  IDs of virtual local area networks (VLAN) that are applied when using VLAN technology in accordance with the IEEE 802.1q standard. When used for an address space rule, the **VLAN ID** parameter may take the following values:

  - **Any** – VLAN technology is used for network interactions between devices, and any VLAN IDs can be used.
  - **Unallowed** – VLAN technology is not used for network interactions between devices.
  - **Any or not used** – VLAN technology is either not used for network interactions between devices, or it is used with any VLAN IDs.
  - **Fixed values** with a list of VLAN IDs – VLAN technology is used for network interactions between devices, and an address space can include only address information that has one of the listed VLAN IDs.

- **IP addresses**.

  IP addresses included in the address space. Addresses can be specified individually, as ranges, or in CIDR subnet address format.

When viewing the rules table, you can use the configuration functions (by clicking the ⚙ icon) and search functions.

About address space subnets

The subnets of address spaces are displayed in the **Subnets** blocks within descriptions of address spaces.

The application checks the detected IP addresses against the list of subnets of address spaces, and can do the following depending on whether the IP addresses belong to specific types of subnets:

- Add a device with its detected IP address to the devices table and monitor the activity of this device.
- Display a device with its detected IP address on the network interactions map and the topology map as its corresponding type of node (known device, unknown device, or WAN node).
- Display a network interactions map link in which one of the sides of interaction is a device with a detected IP address.
- Verify the interaction of a device with a detected IP address based on defined rules (Interaction Control rules, Intrusion Detection rules, and correlation rules).
- Ignore the activity of a device with a detected IP address.

The settings of address space subnets are displayed in the following columns of the table:

- **Subnet**.

  Subnet address in Classless Inter-Domain Routing (CIDR) format: `<base address of subnet>/<number of bits in mask>`. The addresses of subnets are displayed as a tree that shows the nesting hierarchy of subnets.

- **Type**.

  Subnet type that determines its purpose. The following types are provided:

  - **Private, IT** – subnet for devices serving as information technology (IT) resources, such as file servers.
  - **Private, OT** – subnet for devices related to operating technologies (OT), such as PLCs.
  - **Private, DMZ** – subnet for devices residing within a network segment of a demilitarized zone (DMZ), such as servers that handle requests from external networks.
  - **Public** – subnet that is considered to be an external (global) network for devices in other types of subnets. IP addresses from this subnet are represented by a WAN node on the network interactions map.
  - **Link-local** – subnet for network interactions within one segment of the local area network (not routed).

- **Range**.

  Range of IP addresses in the subnet.

- **Ignore MAC addresses**.

  Indicates whether detected MAC addresses are ignored when creating allow rules for network interactions involving IP addresses from the subnet. If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.

- **Automatically add subnets**.

Indicates whether nested subnets are automatically added based on data received from EPP applications. If this mode is enabled, the application adds nested subnets based on data received from EPP applications.

When viewing the subnets table, you can use the configuration functions (by clicking the ⚙ icon), and the filter, search, and sorting functions.

Adding an address space

You can add address spaces to the application if you need to arrange addresses of devices into sets based on a specific attribute (for example, based on the specific network segments of devices).

Maximum number of address spaces in the application – 100.

Only users with the Administrator role can add address spaces.

To add an address space:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Address spaces** tab, open the details area by clicking the **Add AS** button.
4. Enter the name of the address space.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   The address space name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of another address space (not case-sensitive).

   > It is recommended to set an address space name that is no more than 6–8 characters long. If the name contains more characters, the address information may not be fully displayed in the cells of some data tables (for example, in the devices table).

5. If necessary, enter a text description of the address space.
6. Configure the settings of the first address space rule.
7. If necessary, add and configure additional address space rules by clicking the **Add rule** button.

   The total number of rules in an address space cannot exceed 10.

8. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

The lower part of the **Address spaces** tab will show a separate block containing information about the added address space.

Generating a list of subnets for asset management

You can generate lists of subnets for address spaces while taking into account the specific addressing of devices within the network of your organization.

If Kaspersky Industrial CyberSecurity for Networks receives data from EPP applications, the application can use this data to automatically add subnets in the appropriate address spaces. The application automatically adds detected subnets if they are nested within a subnet for which automatic addition of subnets is enabled.

Only users with the Administrator role can generate a list of subnets.

You can use the following functions to generate a list of subnets:

- **Adding a subnet** ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Address spaces** tab, expand the block containing information about the address space in which you want to add a subnet.
4. In the header of the **Subnets** block, click the + icon.

   The details area appears in the right part of the web interface window.
5. In the **Subnet** field, enter the subnet address in CIDR format: `<base address of subnet>/<number of bits in mask>`.
6. In the **Type** drop-down list, select the type of subnet according to its purpose.
7. Set the following toggle buttons to the necessary positions:
   - **Ignore MAC addresses for NIC rules** – enables and disables the mode for skipping detected MAC addresses when creating allow rules based on Network Integrity Control technology.

     If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.
   - **Automatically add subnets** – enables and disables automatic addition of nested subnets according to data received from EPP applications.

     If this mode is enabled, the application adds nested subnets within this subnet based on data received from EPP applications. By default, the type selected for the current subnet is indicated for these nested subnets.
8. Click **Save**.

The list of subnets will show the new subnet at its corresponding level of the hierarchy within the tree.

- **Editing subnet settings** ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Address spaces** tab, expand the block containing information about the address space in which you want to edit the subnet settings.

4. Expand the **Subnets** block and select the relevant subnet.

   The details area appears in the right part of the web interface window.

5. Click the **Edit** button.

6. Depending on the necessary result, perform the following actions:

   - In the **Subnet** field, enter the subnet address in CIDR format: `<base address of subnet>/<number of bits in mask>`.

     The address of the root subnet cannot be edited.

   - In the **Type** drop-down list, select the type of subnet according to its purpose.

     > When changing the subnet type, keep in mind that a new type of subnet may affect the accessible operations that the application can perform with IP addresses from this subnet. For example, if you select the **Public** type, the network interactions map will no longer display links to devices that were assigned IP addresses from this subnet.

   - Set the following toggle buttons to the necessary positions:

     - **Ignore MAC addresses for NIC rules** – enables and disables the mode for skipping detected MAC addresses when creating allow rules based on Network Integrity Control technology.

       If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.

     - **Automatically add subnets** – enables and disables automatic addition of nested subnets according to data received from EPP applications.

       If this mode is enabled, the application adds nested subnets within this subnet based on data received from EPP applications. By default, the type selected for the current subnet is indicated for these nested subnets.

7. Click **Save**.

If the **Subnet** parameter is changed, the tree hierarchy level may be changed for a subnet.

- Deleting subnets ?

In the list of subnets of an address space, you can delete any subnet except the root subnet in the tree (subnet 0.0.0.0/0).

To delete subnets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Assets** section.
3. On the **Address spaces** tab, expand the block containing information about the address space from which you want to delete subnets.
4. Expand the **Subnets** block and select the subnets to delete.

   The details area appears in the right part of the web interface window.
5. Click the **Delete** button.

   A window with a confirmation prompt opens.
6. In the prompt window, confirm deletion of the subnets.

Deleted subnets will no longer be displayed in the list of subnets. If a deleted subnet contained nested subnets, these subnets will remain in the list (but the tree hierarchy level of these subnets will change).

Viewing information about devices with IP addresses from the selected subnets

You can view information about devices with assigned IP addresses from the selected subnets in an address space. Information about devices is displayed in the devices table. The devices table automatically applies a filter based on the addresses of subnets.

To view information about devices in the devices table:

1. Select the **Assets** section.
2. On the **Address spaces** tab, expand the block containing information about the address space containing the relevant subnets.
3. Expand the **Subnets** block and select the subnets for which you want to view information about devices.

   The details area appears in the right part of the web interface window.
4. Click the **Show devices** button.

The **Devices** tab opens in the **Assets** section. The devices table will be filtered based on the IP addresses in the address information of devices.

Changing an address space

You can change the names, text descriptions, and settings of address space rules for added address spaces. These changes cannot be made to the **Default** address space.

You can also generate lists of subnets for any address spaces (including the list of subnets of the **Default** address space).

> When changing the settings of an address space rule, you must take into account the established links between this address space and the addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. If changing the settings in address space rules results in the deletion of links between this address space and addresses, the application automatically deletes these addresses. This could lead to the deletion of application objects (such as devices) if these objects have no other remaining addresses.

Only users with the Administrator role can change the names, text descriptions, and settings of address space rules.

To change the name, text description, or settings of address space rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Address spaces** tab, click the ✎ icon in the block containing information about the relevant address space.

   The details area appears in the right part of the web interface window.

4. Depending on the necessary result, perform the following actions:

   - Enter the name of the address space.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     The address space name must meet the following requirements:

     - Must begin and end with any permitted character except a space.

     - Must contain 255 characters or less.

     - Must not match the name of another address space (not case-sensitive).

     > It is recommended to set an address space name that is no more than 6–8 characters long. If the name contains more characters, the address information may not be fully displayed in the cells of some data tables (for example, in the devices table).

   - Enter a description of the address space.

   - Configure the settings of address space rules.

   - If necessary, add and configure additional address space rules by clicking the **Add rule** button or delete any unnecessary rules by using the × icons.

     The total number of rules in an address space cannot exceed 10.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

6. In the prompt window, confirm the changed address space settings.

Deleting an address space

You can delete address spaces that have been added. You cannot delete the **Default** address space.

> When deleting an address space, you must take into account the established links between this address space and the addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. If deleting an address space results in the deletion of links between this address space and addresses, the application automatically deletes these addresses. This could lead to the deletion of application objects (such as devices) if these objects have no other remaining addresses.

Only users with the Administrator role can delete address spaces.

To delete an address space:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Address spaces** tab, click the 🗑 icon in the block containing information about the address space that you want to delete.

   A window with a confirmation prompt opens.

4. In the prompt window, confirm deletion of the address space.

Configuring Process Control

Kaspersky Industrial CyberSecurity for Networks can monitor an industrial process by tracking process parameters and system commands transmitted in industrial network traffic. The application tracks this data for devices that are displayed in the devices table and that have defined Process Control settings.

Process Control settings can be configured for the types of devices and protocols that are supported by the application.

For automated control of the industrial process, you can employ Process Control rules and system command monitoring functionality. You can also track process parameters in online mode.

A *Process Control rule* is a group of settings that define a condition for the values of a tag. Process Control rules contain descriptions of situations that must be detected in industrial network traffic (for example, when a tag exceeds the specified value).

When the condition defined in a rule is fulfilled, an event is registered by Kaspersky Industrial CyberSecurity for Networks. You can define the relevant event registration settings (for example, headers of events) when configuring Process Control rules.

Monitoring system commands ensures registration of events when transmitted system commands are detected in traffic. When configuring Process Control settings for devices, you can select the relevant system commands to monitor. This functionality can be used regardless of Process Control rules.

Only users with the Administrator role can configure Process Control settings for devices and generate lists of monitored tags and Process Control rules. However, data can be viewed and exported by users with the Administrator or Operator roles.

You can generate lists of monitored tags and Process Control rules on the Server web interface page in the **Process control** section. You can configure Process Control settings for devices when working with the devices in the **Assets** section and **Network map** section.

Supported devices and protocols

Kaspersky Industrial CyberSecurity for Networks analyzes traffic of the following types of devices used for process automation:

- **Programmable logic controllers (PLC)** ?

- ABB™ AC 700F, 800M
- ABB B&R
- Allen-Bradley® ControlLogix®, CompactLogix™ series
- AutomationDirect DirectLOGIC
- BECKHOFF® CX series
- Emerson DeltaV MD, MD Plus, MQ
- Emerson ControlWave series
- General Electric RX3i
- Honeywell C300 for Experion PKS / PlantCruise control systems
- Honeywell ControlEDGE 900 series
- IPU950
- Mitsubishi System Q E71
- OMRON CJ2M
- Schneider Electric Foxboro FCP270, FCP280
- Schneider Electric Modicon: M580, M340, Momentum
- Siemens SIMATIC® S7-200, S7-300, S7-400, S7-1200, S7-1500
- YCU and ELC supporting the YARD protocol
- Yokogawa CENTUM
- Yokogawa ProSafe-RS
- OWEN PLC100 series
- Prosoft-Systems Regul R500
- KNX® devices
- Devices in Valmet DNA control systems
- Devices that support the Allen-Bradley EtherNet/IP protocol
- Devices supporting the COS protocol
- Devices supporting the DTS protocol
- Devices supporting the FEU protocol

  - Devices supporting the PK4 protocol
  - Devices supporting the PNU20 protocol
  - Devices supporting the CODESYS V2 and V3 protocols
  - Devices that support the Siemens S7comm and S7comm-plus protocols
  - Devices that support PROFINET IO standard protocols

- Intelligent electronic devices (IED) ?

  - ABB Relion™ series: REF615, RED670, REL670, RET670
  - General Electric Multilin series: B30, C60
  - MiCOM C264
  - Schneider Electric P545
  - Schneider Electric Sepam 80 NPP series
  - Siemens SIPROTEC™ 4: 6MD66, 7SA52, 7SJ64, 7SS52, 7UM62, 7UT63
  - Relematika TOR 300
  - EKRA 200 series, BE2502, BE2704
  - Devices supporting the DNP3 protocol
  - Devices supporting the Schneider Electric UMAS protocol
  - Devices supporting protocols of the IEC 60870 standard: IEC 60870-5-101, IEC 60870-5-104
  - Devices supporting protocols of the IEC 61850 standard: IEC 61850-8-1 (GOOSE, MMS), IEC 61850-9-2 (Sampled Values)
  - Devices supporting the Modbus TCP protocol

- Devices with server software installed ?

- FTP server
- OPC DA server
- OPC UA server
- Siemens SICAM PAS server
- TASE.2 server
- Server with encryption support
- ARMS SCADA system devices

- Devices categorized as network equipment ?
  - Moxa NPort series
  - I/O devices that support the following protocols: BACnet™, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, WMI device interaction protocol, and OPC UA Binary

Kaspersky Industrial CyberSecurity for Networks also has *generic types* of devices for process control: **Generic PLC**, **Generic IED** and **Generic Gateway**. Using these types of devices, you can configure Kaspersky Industrial CyberSecurity for Networks to analyze traffic for those devices that are not on the list of supported types. For generic types of devices, you can specify any combination of application-level protocols from the list of supported protocols on devices related to programmable logic controllers, intelligent electronic devices and network gateways.

For the supported types of devices, Kaspersky Industrial CyberSecurity for Networks analyzes communications over the following application-level protocols:

- ABB™ SPA-Bus
- Allen-Bradley EtherNet/IP
- BECKHOFF® ADS/AMS
- BSAP
- CODESYS V2 and V3 Gateway over TCP and V3 Gateway over UDP
- COS
- DMS for ABB AC 700F devices
- DNP3
- Emerson ControlWave Designer
- Emerson DeltaV, including the protocol for updating embedded software (firmware)
- FTP

- General Electric EGD
- General Electric SRTP
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104
- IEC 61850: GOOSE, MMS (including MMS Reports), Sampled Values
- INA2000
- KNXnet/IP
- Mitsubishi MELSEC System Q
- MMS (ISO 9506-2)
- Modbus TCP
- OMRON FINS
- OPC DA, protocol for interaction of devices over WMI technology
- OPC UA Binary
- PROFINET IO and RPC for PROFINET IO
- Schneider Electric UMAS
- Siemens Industrial Ethernet
- Siemens S7comm, S7comm-plus
- TASE.2
- YARD
- Yokogawa Vnet/IP
- Relematika BDUBus
- PK4
- PNU20
- Modification of the Modbus TCP protocol for devices of Ekra 200 series
- Automated radiation monitoring systems (ARMS) protocol
- Protocol for interaction between Siemens SICAM PAS and SICAM SCC (based on SIMATIC WinCC)
- AutomationDirect DirectLOGIC device interaction protocol
- Protocol for interaction of Foxboro FCP270, FCP280 devices
- IPU-FEU device interaction protocol

- MiCOM C264 device interaction protocol
- Valmet DNA device interaction protocol
- Protocol for initial setup of Prosoft-Systems devices
- DTS data transfer protocol
- Protocol of devices with Siemens DIGSI 4 system software
- Protocols for interaction of devices in Honeywell Experion PKS / PlantCruise control systems
- Protocols for initial configuration and interaction of Moxa NPort series devices
- Protocols for detection and interaction of Honeywell ControlEDGE 900 series devices

To analyze traffic and interactions of devices, the application uses specialized modules for processing application-level protocols. The modules included in packages from the Kaspersky Industrial CyberSecurity for Networks distribution kit provide support for the listed types of devices and application-level protocols. You can update protocol processing modules by installing updates. When installing updates to the application, new modules that support additional types of devices and/or application-layer protocols may be added.

Kaspersky Industrial CyberSecurity for Networks also analyzes traffic transmitted over common protocols. For a list of the supported common protocols, see the Appendix.

Process Control devices

For industrial process control purposes, you can use devices from the devices table that have Process Control settings defined.

Kaspersky Industrial CyberSecurity for Networks supports the use of various types of devices and application-layer protocols for Process Control.

You can view and edit Process Control settings in the details area of the device selected in the **Assets** section or in the **Network map** section of the Kaspersky Industrial CyberSecurity for Networks web interface.

Process Control settings for devices

Process Control settings for devices are displayed in the details area when a device is selected in the devices table, on the network interactions map, or on the topology map. If the process control settings are set for the device, the **Process Control settings** tab in the details area contains the following information:

- **Device type** – type of device from the list of device types supported for Process Control.
- **Protocol** – name of the utilized protocol. The following information is displayed for each protocol:
  - **System commands** – main settings for tracking system commands for a protocol. This field shows the total number of system commands for the protocol and the number of monitored system commands that will cause the application to register events if detected.
  - Address information – depending on the selected protocol, this field contains the IP address and port, MAC address or domain ID (for the IEC 61850: GOOSE protocol). If additional address spaces were added to the

application, the specific address space must be indicated for an address (and the OSI model layers selected for address space rules must match the address).

- Additional settings depending on the selected protocol. Additional settings are displayed if the application lets you configure more than system commands and address information for this protocol.

> Examples:
> When the Modbus TCP protocol is selected, the additional setting **Reverse order of registers** is also displayed. This setting lets you enable or disable support for an inverted sequence of registers (machine words) in 32-bit data values.
>
> When the IEC 60870-5-101 protocol is selected, the following additional settings are displayed:
>
> - **Two-byte ASDU address** – lets you enable or disable two-byte addressing mode for application service data units (ASDU). If this mode is disabled, one-byte addressing is used.
> - **Originator** – lets you enable or disable the use of an additional byte for the originator's address in the data block ID.
> - **Channel address block (bytes)** – number of bytes in a data link layer address block.
> - **Object address block (bytes)** – number of bytes in an information object address block.

You can add Process Control settings for devices in the following ways:

- Automatically
- Manually
- Import from external projects

About automatic detection of Process Control settings for devices

Kaspersky Industrial CyberSecurity for Networks can automatically identify the Process Control settings for devices and save these settings in the device information. Settings are identified by analyzing traffic to detect the protocol commands for devices involved in the industrial process.

The application automatically adds or edits Process Control settings for devices that have been added to the devices table. Devices can also be automatically added to the devices table if the Device Activity Detection method is enabled for Asset Management.

Automatically added Process Control settings are considered to be *system* settings. The application can change these settings if protocol commands with updated parameter information are detected in traffic.

Process Control settings that are manually added by a user are considered to be *custom settings*. The application does not change user-defined Process Control settings. If a user manually changes system settings for Process Control, these settings will also become custom settings.

Automatic detection of the Process Control settings for devices is performed when the Device Discovery for Process Control method based on the Deep Packet Inspection technology is used. You can enable and disable this method.

To automatically detect Process Control settings, the application employs modules for processing application-layer protocols. The application is installed with built-in modules that can determine the main settings for a number of devices and protocols that are indicated on the list of types of devices and protocols supported by the application. You can update protocol processing modules by installing updates.

Manually adding Process Control settings for a device

You can manually add Process Control settings for a device when working with the devices table, the network interactions map, or the topology map. Process Control settings that were added for a device are considered to be custom settings. User-defined settings are not changed when Process Control settings are automatically detected for devices.

Only users with the Administrator role can add Process Control settings.

To add Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the relevant asset in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Add**.

   The **Add Process Control settings** window appears.

4. Configure the Process Control settings:

   a. Select the device type.

   b. Select the protocol used for interaction with the device within the industrial process.

   c. If necessary, edit the settings for monitoring system commands over the selected protocol. By default, the application monitors all system commands except those that are frequently encountered during normal operation of the device.

   d. If you need to configure other settings for the selected protocol (such as address information for interaction with the device), specify the relevant values in the fields that appear.

   e. If you want to additionally specify a different protocol (that is supported for the selected device type) or a different combination of settings for a previously selected protocol (when using multiple connected modules within one device), add the settings for this protocol by clicking the **Add protocol** link.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process Control settings** tab, in the details area, a dedicated section with the specified parameters is displayed.

Editing Process Control settings for a device

If Process Control settings were added for a device, you can manually edit these settings when working with the devices table, the network interactions map, or the topology map. After saving the changes, Process Control settings for a device are considered to be custom settings. User-defined settings are not changed when Process Control settings are automatically detected for devices.

Only users with the Administrator role can edit Process Control settings.

To edit Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the relevant asset in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Edit**.

   The **Edit Process Control settings** window appears.

4. Configure the Process Control settings. You can edit individual settings (for example, edit the settings for tracking system commands for a specific protocol) or reconfigure all settings in the same order as you would when adding Process Control settings.

   > When you edit settings that were used in previously created tags, the application automatically deletes these tags and their associated Process Control rules. For example, if you delete a protocol, after saving the settings the application will delete all tags containing the device and deleted protocol (the Process Control rules associated with these tags will also be deleted).

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process Control settings** tab, in the details area, the information in the section with the defined parameters is refreshed.

Selecting the monitored system commands

You can configure traffic monitoring of system commands that are transmitted and received by process control devices.

In Kaspersky Industrial CyberSecurity for Networks, system commands include management commands (for example, START PLC) as well as system messages related to the operation of devices or containing packet analysis results (for example, REQUEST NOT FOUND). System commands in Kaspersky Industrial CyberSecurity for Networks are categorized based on the categories listed in the Appendices.

When a monitored system command is detected, Kaspersky Industrial CyberSecurity for Networks registers an event for Command Control technology. The event is registered using the system event type that is assigned the code 4000002602. You can configure the settings for this type of event.

Only users with the Administrator role can configure monitoring of system commands for devices.

To configure monitoring of system commands for a device:

1. In the **Assets** section on the **Devices** tab or in the **Network map** section, select the relevant device with defined Process Control settings.

   In the **Network map** section, you can select the device on both the network interactions map and the topology map.

   If Process Control settings are not defined for a device, add the settings.

2. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Edit**.

   The **Edit Process Control settings** window appears.

3. Specify the relevant system commands for the first protocol. To do so, expand the **System commands** list under the **Protocol** field and select the check boxes of the system commands that you want to monitor. After selecting system commands, click **OK**.

4. If a different protocol is additionally indicated in the Process Control settings, or if it is the same protocol but with different address information, select the system commands that will be monitored during communications over this protocol. To do so, use the **System commands** drop-down list under the field containing the name of this protocol. Likewise, configure monitoring of system commands for all other specified protocols of the device.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process Control settings** tab, in the details area, the information in the section with the defined parameters is refreshed.

Clearing Process Control settings defined for a device

You can clear Process Control settings for a device when working with the devices table, the network interactions map, or the topology map.

> When clearing Process Control settings defined for a device, the application automatically deletes all tags that were created for this device. In addition to the tags, all of their associated Process Control rules are also deleted.

Only users with the Administrator role can clear Process Control settings for a device.

To clear Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the relevant asset in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Delete**.

   A window with a confirmation prompt opens.

4. In the prompt window, confirm deletion of the settings.

The Process Control settings section is deleted from the **Process Control settings** tab in the details area.

Importing configurations of devices and tags from external projects

Configurations of Process Control settings for devices and tags can be imported into Kaspersky Industrial CyberSecurity for Networks from external project files. In the context of Kaspersky Industrial CyberSecurity for Networks, *external projects* are projects that contain data on devices and tags saved by other systems (such as a SCADA ? system).

To import files of external projects, the files must be packed into a ZIP archive (except for files of certain projects whose contents consist of a ZIP archive).

Supported types of projects for importing ?

Configurations of devices and tags can be imported from data files comprising the following types of projects:

- Universal-format project.

  This type of project can be obtained from any source by converting and saving its data in text files with delimiters in CSV format. For information about files in a universal project, please refer to the Appendices.

- AC 800M configuration file for OPC server.

  This type of project can be obtained via ABB AC 800M device management software.

- Control Builder M project.

  This type of project can be obtained via ABB Control Builder M software.

- COS device configuration archive.

  This type of project can be obtained via device management software for devices supporting the COS protocol.

  > Configuration files of devices do not contain the network IP addresses that are used by these devices. After adding devices from configuration files, you will need to verify the information about devices in the application and manually define the correct IP addresses for these devices if necessary.

- DeltaV project.

  This type of project can be obtained via Emerson DeltaV device management software.

- DirectSOFT6 project.

  This type of project can be obtained via DirectLOGIC device management software.

- ABB Freelance 2016 Engineering tag list.

  This type of project can be obtained via ABB Freelance 2016 Engineering software.

- Project for IEC 61850 devices.

  This type of project can be obtained via device management software for devices supporting IEC 61850 standard protocols.

- RSLogix 5000® project (provided as a CSV- or ACD file).

  This type of project can be obtained via RSLogix 5000 device management software.

  > When importing a CSV file containing an RSLogix 5000 project, the application ignores structural and custom types of tags in this project. If you want to add these tags to the application, you can import an ACD file containing the RSLogix 5000 project or enable Unknown Tag Detection to add tags from traffic.

- SICAM PAS V7 project (represented by a description TXT file or a PXD file).

  This type of project can be obtained via Siemens SICAM PAS version 7 software.

- TIA Portal V12/V13 project.

  This type of project can be obtained via Siemens TIA Portal version 12 or 13 software.

- Schneider Electric Unity project.

This type of project can be obtained via Schneider Electric Modicon device management software. A project can be provided as ZEF- or XEF files (if a project is provided as a ZEF file, this file does not need to be packed into a ZIP archive for import).

> When a Schneider Electric Unity project is imported, the added devices are assigned the names of the files from which they were imported. You can manually define names for these devices when editing device information.

- WinCC® project (including WinCC OA, WinCC flexible).

  This type of project can be obtained via Siemens SIMATIC WinCC, WinCC OA, or WinCC flexible software.

- YARD configuration file.

  This type of project can be obtained via device management software for devices supporting the YARD protocol.

- CIMPLICITY export CSV file.

  This type of project can be obtained via CIMPLICITY software.

- Valmet DNA configuration file.

  This type of project can be obtained via Valmet DNA software.

- EGD configuration XML file.

  This type of project can be obtained by exporting a configuration for data exchange via the General Electric EGD protocol.

- ControlWave project SIG-file.

  This file is included in the project used by Emerson ControlWave series devices.

- Honeywell Control Builder project.

  This type of project can be obtained via Honeywell Control Builder software.

- PcVue V10/V11 project

  This type of project can be obtained via PcVue version 10 or 11 software.

- Proficy export CSV file.

  This type of project can be obtained via Proficy software.

- Foxboro IACC export file project.

  This type of project can be obtained via Foxboro IACC software.

- PNU20 configuration file.

  This type of project can be obtained via device management software for devices supporting the PNU20 protocol.

You can update and expand the supported types of projects by installing updates.

To import configurations of devices and tags from an external project:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Devices** tab in the toolbar above the devices table, open the **Import** drop-down list.

4. In the drop-down list, select the option with the relevant project type.

   The **Importing <project type>** window will appear on the screen.

5. In the **File to import** field, select the project file with the **Browse** button.

6. Select the relevant option for your existing configurations of devices and tags. To do so, click one of the following buttons:

   - **Add** means that the imported configurations of devices and tags will be added to the existing configurations of devices and tags.

   - **Replace** means that the existing configurations of devices and tags, associated with those devices for which new configurations and tags are imported, are deleted (tags with user-defined process control rules are not deleted).

7. Confirm the import by clicking **Continue**.

   The data import process starts. Information about the running import operation is displayed in the list of background operations. When the process completes, the imported configurations of devices and tags will be available for upload in the devices table and tags table.

8. If you want to view a report on the results of the import:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the import operation to complete.

   c. Click the **Display report** button.

Tags

A *tag* is a process parameter transmitted in the industrial network (for example, a controlled temperature). The values of tags are transmitted and received by devices over specific protocols.

You can add tags to the application in the following ways:

- Manually

- Automatically when unknown tags are detected

- Importing from external projects

A tag can be added under the following conditions:

- The devices table contains a device associated with the tag being added.

- A device has defined Process Control settings in which the protocol of the added tag is indicated.

After adding a tag to the application, this tag can be used in Process Control rules. In accordance with the conditions defined in Process Control rules, the application will register the corresponding events in which the received tag values may be saved.

You do not need to add this tag to Process Control rules to control tag values when monitoring process parameters.

You can view and edit tags in the **Process Control section of** the **Tags** tab.

About Unknown Tag Detection

Kaspersky Industrial CyberSecurity for Networks can analyze traffic to detect and save information about unknown tags. Unknown tags are tags that are absent from the tags table.

The application adds a detected tag to the tags table if the conditions for adding a tag are fulfilled. If one of the conditions is not fulfilled, the detected tag is ignored (for example, if the tag has no associated protocol specified for the device in the Process Control settings).

Information about unknown tags is received from traffic using the Unknown tag detection method based on the Deep Packet Inspection technology. You can enable and disable this method.

> When the Unknown Tag Detection method is used, the performance of application-layer protocol processing modules may be slightly reduced. For this reason, Unknown Tag Detection is disabled by default after the application is installed. It is recommended to enable the Unknown Tag Detection method for a period of time sufficient to detect all tags that may be associated with devices with the specified Process Control settings. It is recommended to disable this method after the detected tags are added to the table.

Unknown Tag Detection is supported for the following protocols:

- Allen-Bradley EtherNet/IP
- BACnet
- BSAP
- CODESYS V3 Gateway
- DMS for ABB AC 700F devices
- DNP3
- Emerson DeltaV
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104
- IEC 61850: MMS
- Modbus TCP
- OPC DA
- OPC UA Binary

- Schneider Electric UMAS
- Siemens S7comm
- TASE.2
- Yokogawa Vnet/IP
- PNU20
- Protocol for interaction of Foxboro FCP270 and FCP280 devices

Manually adding a tag

Only users with the Administrator role can manually add tags.

To manually add a new tag:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Tags** tab, open the details area by clicking the **Add tag** button.
4. Click the **Select device** link to open the device selection window.
5. In the device selection window, select the device for which you want to create a tag and click **OK**.

   The device selection window contains a table in which you can configure the layout and order of columns, and filter, search, and sort similarly to the devices table in the **Assets** section.
6. Select the protocol that is indicated in the Process Control settings for the selected device. You must select a protocol that supports the transmission of tags.

   If the necessary protocol is not available, you can configure the Process Control settings and specify the necessary protocol. To open the settings window, use the button on the right of the protocol selection field. Process Control settings are configured the same as when adding or editing settings while working with the devices table.
7. Change the tag name if necessary. The default name according to the template is **Tag <value of the device tag counter>**.

   You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The tag name must begin and end with any permitted character except a space.
8. Configure other tag parameters.

   The mandatory parameters (such as the tag name and data type) must be specified for a tag. Depending on the selected protocol and data type, additional parameters (such as the unit of measure and scaling limits) may be available for configuration.
9. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

The new tag appears in the tags table.

Editing tag parameters

Only users with the Administrator role can edit tag parameters.

To edit tag settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Tags** tab, select the relevant tag.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.
5. Change the tag name if necessary.

   You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The tag name must begin and end with any permitted character except a space.
6. Configure other tag parameters.

   The mandatory parameters (such as the tag name and data type) must be specified for a tag. Depending on the selected protocol and data type, additional parameters (such as the unit of measure and scaling limits) may be available for configuration.
7. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

Adding tags to the favorites list

If you want to create a list of the most important tags and quickly navigate to this list (for example, to view the current values of these tags), you can add tags to the favorites list. Tags can be added to the favorites list and deleted from it at your own discretion. The number of tags on the favorites list is unlimited.

To display the list of favorite tags, you can filter by the **Favorites** column when viewing the tags table.

A created tag is not add to the favorites list by default.

To add tags to the favorites list:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Tags** tab, select the tags that you want to add to the favorites list.
4. Right-click to display the context menu of one of the selected tags.

5. Do one of the following:
   - If you have selected one tag, add it by clicking the **Add tag to favorites list** option in the context menu.

     This option is not displayed in the context menu if the selected tag has already been added to the favorites list.
   - If you have selected multiple tags, add them by clicking the **Add tags to favorites list** option in the context menu.

     This option is not displayed in the context menu if all selected tags have already been added to the favorites list.

     If all tags that satisfy the current filter and search settings are selected, and the number of selected tags is more than 1,000, the application does not check whether the tags are on the favorites list. In this case, the **Add tags to favorites list** option is always displayed in the context menu.

   In the tags table, **Yes** is displayed for all selected tags in the **Favorites** column.

To delete tags from the favorites list:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Tags** tab, select the tags that you want to remove from the favorites list.
4. Right-click to display the context menu of one of the selected tags.
5. Do one of the following:
   - If you have selected one tag, remove it by clicking the **Remove tag from favorites list** option in the context menu.

     This option is not displayed in the context menu if the selected tag has already been removed from the favorites list.
   - If you have selected multiple tags, remove them by clicking the **Remove tags from favorites list** option in the context menu.

     This option is not displayed in the context menu if all selected tags have already been removed from the favorites list.

     If all tags that satisfy the current filter and search settings are selected, and the number of selected tags is more than 1,000, the application does not check whether the tags are on the favorites list. In this case, the **Remove tags from favorites list** option is always displayed in the context menu.

   In the tags table, **No** is displayed for all selected tags in the **Favorites** column.

Deleting tags

Only users with the Administrator role can delete tags.

To delete tags:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Process Control** section.

3. On the **Tags** tab, select the tags that you want to delete.

4. On the toolbar located above the tags table, click the **Delete** button.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm deletion of the tags.

Process Control rules

The application can employ the following Process Control rules to monitor the values of tags:

- Rules with defined conditions. These rules contain conditions for tracking the values of tags. Each rule can contain one of the provided types of conditions. If a condition defined in a rule is fulfilled, the application registers an event. The settings of a registered event are also defined in the rule.

- Rules with Lua scripts. These rules contain descriptions of algorithms used for checking the values of tags. The algorithms are compiled in the Lua programming language using functions and variables for Lua scripts. When an algorithm in a rule containing a Lua script is triggered, the application registers an event (the settings of a registered event are defined in the rule). If you are using Lua scripts for Process Control rules, you can use a *global Lua script* in which the global Lua variables and functions are initialized. You can use these global variables and functions in a Lua script of any rule. By default, the global Lua script is empty and does not contain executable code. The application can have only one global Lua script at one time.

The application applies Process Control rules when using the rule-based process control method based on the Deep Packet Inspection technology. You can enable and disable this method.

Process Control rules can be enabled or disabled. Enabled rules are applied during traffic analysis. Disabled rules are not applied and are not taken into account.

The application can automatically create Process Control rules with defined conditions when Process Control is running in learning mode.

You can view and edit Process Control rules in the **Process Control** section on the **Rules** tab.

Rules with defined conditions for tag values

To monitor the values of tags, you can employ Process Control rules in which conditions are defined for the values of tags. Each rule can contain one of the provided types of conditions. A rule can be bound to only one tag. However, you can create up to 20 rules with different types of conditions for one tag.

Rules with defined conditions can be created automatically by the application when Process Control is running in learning mode. You can also manually create and edit rules with defined conditions for the values of tags.

For a Process Control rule, you can select one of the following types of conditions:

- **Value changed** – the value of the controlled tag was either completely changed or was changed in a specific bit.

If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of any type of tag. You can also specify the number of saved (allowed) values of a tag whose detection will not result in the registration of an event. For a rule, you can specify a number of saved values from 1 to 10 (the saved values will be updated as new values are detected). By default, only the latest value is saved.

If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64).

- **Tag missing** – the controlled tag was not detected in monitored traffic during the defined time period.

  You can use this condition to monitor any type of tag.

- **Detection** – the controlled tag was detected in the traffic being monitored.

  You can use this condition to monitor any type of tag.

- **In range** – the value of the controlled tag is inside the specified range.

  You can use this condition to monitor only int and float tags.

  You can define values for the lower and/or upper limit of the range. The defined values for limits can be included in the range or excluded from it.

- **Out of range** – the value of the controlled tag is outside of the specified range.

  You can use this condition to monitor only int and float tags.

  You can define values for the lower and/or upper limit of the range. The defined values for limits can be included in the range or excluded from it.

- **Equals** – the value of the controlled tag is equal to one of the defined values, either completely or in a specific bit.

  If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of int, bool and string tags. You can define from 1 to 10 values for comparison.

  If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64) and the value of the bit for comparison (indicated as one of two integers: zero or one).

- **Does not equal** – the value of the controlled tag is not equal to one of the defined values, neither completely nor in a specific bit.

  If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of int, bool and string tags. You can define from 1 to 10 values for comparison.

  If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64) and the value of the bit for comparison (indicated as one of two integers: zero or one).

- **Monotonic change violation** – the value of a controlled tag violates the sequence of monotonic increase or reduction of values.

  You can use this condition to monitor only int and float tags.

For rules that monitor the values of tags, you need to take into account how the application processes values represented by denormalized numbers (low-order numbers approaching zero – for example, 2.22507e-308 if this value is represented with double precision). The application converts denormalized numbers into zero values.

For any condition, you can select the operations for which the application will monitor the values of a tag. The following monitoring options are available depending on operations performed with the tag:

- **Monitor when reading tag** – the value is checked when reading a tag from a device.
- **Monitor when writing tag** – the value is checked when writing a tag to a device.

Rules with Lua scripts

Scripts written in the Lua programming language can be used to describe the algorithms for checking the values of tags in Process Control rules. Lua scripts provide the capabilities to not only check the values of tags but also to add various information to registered events and process logs.

A Lua script must consist of one or more functions. The names of the functions must be unique among all rules with Lua scripts. A function that is used to track the values of tags is called a *trigger function*. A trigger function must return a value of `true` to register an event.

If a variable is indicated in a script, the variable must be initialized either in that specific script (to be applied only in that script) or in a separate global script (to be applied in all rules with Lua scripts). A global script can also contain auxiliary functions that can be used in rules with Lua scripts.

A trigger function is called whenever the value of any tag used in the function is changed. The function is first called when all values of tags used in the function are received.

To obtain the values of a tag, the code of a function contains an entry that looks as follows:

```
tag' main_tag_parameters [: field_name ][@ modifier ]'[. transmission_direction ]
```

where:

- `main_tag_parameters` are the mandatory parameters that identify the tag in the application. Parameters are separated by a colon. The main parameters consist of the following parameters from the tags table:
  - **Device**
  - **Tag name**
  - **Tag ID**
- `field_name` is the name of the field within the tag field structure represented by the **Structural values** parameter in the tags table. If a field is embedded into other fields, its name is indicated together with the names of all parent fields separated by a colon. If the `field_name` parameter is not specified, the main value within the tag field structure is checked.
- `modifier` defines how the obtained value is presented. The following modifiers are available:
  - `str` means that the obtained value is converted into a string value.
  - `type` means that the name of the data type from the obtained value is passed as the value.
  - `loc` means that the passed value is the assigned localized name for the obtained value (if there is no localized named, the obtained value is converted into a string value).

If a modifier is not specified, the actual obtained value is used. In this case, the data type of the value is not changed.

- `transmission_direction` defines the direction in which the obtained value is transmitted. The transmission direction can be defined by one of the following parameters:
  - `R` means that the value was received when it was read from a device.
  - `W` means that the value was received when it was written to a device.
  - `RW` refers to any direction of the obtained value.

  If the transmission direction is not defined, the value obtained from any direction is used.

Records for obtaining the values of tags can be used in expressions (for example, assigning values to variables or comparing values).

To perform various operations with a Lua script, you can use *auxiliary functions* supported by the Server. The names of auxiliary functions begin with an underscore (`_`).

The main auxiliary functions for adding information via Lua scripts are as follows:

- Function for adding parameters to use as additional variables in events:

  `_AddEventParam(' parameter_name ', parameter_value )`

  Any name and value can be defined for a parameter. To use a parameter and its value in events, this parameter must be specified in event type parameters as follows: `$extra.< parameter_name >`.

- Functions for adding entries to the process log in which the Lua script is executed (this is normally a process whose name starts with the word `Filter`). A record defined by an argument of the function (variable or constant) is added to the log:
  - To create a record with the *Errors* level:

    `_WriteErrorLog( function_argument )`
  - To create a record with the *Warning* level:

    `_WriteWarningLog( function_argument )`
  - To create a record with the *Info* level:

    `_WriteInfoLog( function_argument )`
  - To create a record with the *Debug* level:

    `_WriteDebugLog( function_argument )`
  - To create a record with the *Debug* level that may contain multiple arguments of the function:

    `print( function_argument1 , function_argument2 ,…)`

    Variables or constants defined by function arguments are separated by a tab character in a log record.

  Records are not created in the log if the level of the record is lower than the logging level set for the process.

Process Control rules learning mode

In Process Control rules learning mode, the application automatically generates Process Control rules with conditions for the values of tags. To generate rules, the application analyzes traffic to monitor the values of only those tags that have been added to the tags table.

Process Control rules that were automatically added in learning mode are called *system* rules. For these rules, the **Origin** parameter contains the **System** value. When system rules are automatically created, the default value of 6.0 is assigned to the **Event score** parameter.

Rules that were manually created are called *User* rules. For these rules, the **Origin** parameter contains the **User** value. If a system rule is manually changed, this rule also becomes a user rule.

The application assigns the *Disabled* status to rules added in the learning mode. If a system rule was updated in the learning mode, this rule remains with the same status as before the update: *Enabled* or *Disabled*.

When adding or updating Process Control rules in learning mode, the application defines one of the following conditions for them:

- **Does not equal**.

  This condition is defined when a rule is added if no other system rule is found for the detected tag value or if up to ten different tag values are received (except for the tags with the bool or float data type).

- **Out of range**.

  This condition replaces the previous condition in a rule if a new value for a tag with the float data type is received or if more than ten different values for a tag with the int data type are received.

- **Monotonic change violation**.

  This condition replaces the previous condition in a rule if the detected tag values have only increased or only decreased, without any other variation. This condition replaces the previous condition in rules for tags with the int or float data type when learning mode ends.

In learning mode, the application also deletes system Process Control rules in the following cases:

- The rule was created for a tag with the bool data type, and the detected and saved values do not match (comparisons are conducted only for the first ten detected values, and all other values are ignored).

- The rule was created for a tag with the string data type, and more than ten different values are received.

You can configure the learning mode for the rule-based process control method.

Process Control rules learning mode must be enabled for a sufficient amount of time to detect all possible values of relevant tags. This amount of time depends on how frequently tags are circulated in traffic, how often devices are running in the industrial network, and other specifics of the industrial process. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period ranging from one to several days to accumulate the maximum amount of data.

Viewing the table of Process Control rules

The Process Control rules table is displayed in the **Process Control** section on the **Rules** tab. The table provides the general settings of rules and of the tags and devices associated with the rules.

The settings of rules are displayed in the following columns of the table:

- **Rule ID**

  Unique ID of the rule.

- **Device group**

  Name of the group containing the device associated with the tag (contains the name of the group and the names of all its parent groups in the device group tree).

- **Device**

  Name of the device associated with the tag.

- **Protocol**

  Name of the protocol used to transmit the tag.

- **Tag name**

  Defined name of the tag for which the rule was created.

- **Rule**

  Defined name of the rule.

- **Rule description**

  Defined description of the rule.

- **Status**

  Current status of the rule (*Enabled* or *Disabled*).

- **Created**

  The date and time when the rule was created.

- **Changed**

  The date and time when the rule was last modified.

- **Condition type**

  Selected type of condition for the rule.

- **Event title**

  Header of the event registered when the rule is triggered.

- **Event score**

  Assessed score of the event that was registered when the rule was triggered. Events are scored on a scale from 0.0 to 10.0.

- **Event description**

  Description of the event registered when the rule is triggered.

- **Origin**

  Information about the origin of the rule.

When viewing the rules table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Creating a Process Control rule with settings of conditions

The following options are provided for creating Process Control rules with settings of conditions:

- Create a new rule for a tag.
- Create an additional rule based on an existing rule.

To create a new rule for a tag:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Tags** tab, select the tag for which you want to create a Process Control rule.

   The details area appears in the right part of the web interface window.
4. In the upper right corner of the details area, click the **Create rule** button.

   This opens the **Rules** tab containing the details area for the created Process Control rule.
5. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

      You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The rule name must begin and end with any permitted character except a space.

   c. Select the type of condition and configure the settings depending on the selected type.

   d. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).
6. Click **Save**.

To create an additional Process Control rule based on an existing rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Process Control** section.
3. On the **Rules** tab, select the rule that you want to use as the basis for creating another rule for the same tag.

   The details area appears in the right part of the web interface window.
4. Click the **Create another rule** button.

   You will see the details area for the created Process Control rule. For the new rule, you will see information about the device, protocol and tag received from the settings of the selected rule.
5. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

   c. Select the type of condition and configure the settings depending on the selected type.

   d. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).

6. Click **Save**.

Creating a Process Control rule with a Lua script

To create a rule with a Lua script:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Process Control** section.

3. On the **Rules** tab, open the details area by clicking the **Add Lua script** button.

4. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

   c. If you want to define the script from a template, in the details area click the **Use Lua template** button, select the necessary template in the opened window and click **Apply**.

   d. In the **Lua script for rule** field, enter the code of the script in the Lua language.

   The script input field displays the names of functions and comments loaded from template. You can create a script by editing and augmenting template strings. When entering text, suggestions or available values automatically appear near the cursor (for example, relevant names of devices and tags when entering settings that identify a tag).

   If the script code does not fit into the **Lua script for rule** field, you can use the ⤢ button to open a separate window for displaying the code.

   e. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).

5. Click **Save**.

Editing Process Control rule settings

To edit Process Control rule settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Process Control** section.

3. On the **Rules** tab, select the rule that you want to edit.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

5. Change the settings as necessary. You can edit the settings by using the same operations that were available when creating Process Control rules with conditions or Lua scripts.

Creating, viewing and editing a global Lua script

Variables and functions defined in a global Lua script can be used in rules with Lua scripts.

Only users with the Administrator role can create or edit a global Lua script for Process Control rules. However, users with the Administrator role and users with the Operator role can both view the contents of a global Lua script.

To create or edit a global Lua script:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Process Control** section.

3. On the **Rules** tab, open the global Lua script editing window by clicking the **Global Lua script** button.

4. Enter the code of the script in the Lua language.

5. Click **Save**.

Deleting Process Control rules

To delete Process Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Process Control** section.

3. On the **Rules** tab, select the rules that you want to delete.

4. Click the **Delete** button. If the button is not displayed on the toolbar, click the ⋮ button and select the desired item in the menu that opens.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm deletion of the rules.

Configuring Interaction Control

Kaspersky Industrial CyberSecurity for Networks can monitor the network interactions of devices in the industrial network. *Interaction Control rules* are used to define authorized and unauthorized network interactions. All detected network interactions that do not satisfy the active Interaction Control rules are considered to be unauthorized. The application registers the corresponding events when unauthorized interactions are detected.

An Interaction Control rule can be applied by one of the following technologies:

- Network Integrity Control – the rule describes network interaction between devices using a specific set of protocols and connection settings.
- Command Control – the rule describes the monitored system commands during communications between devices over one of the supported protocols for Process Control.

An Interaction Control rule contains the following information about interactions/communications:

- Sides participating in network interactions.
- Allowed protocol or system commands.

Network interactions between devices are identified based on the MAC- and/or IP addresses of the devices. If additional address spaces were added to the application, you can configure Interaction Control rules for the addresses of relevant address spaces.

When analyzing network interactions for Network Integrity Control, the application also checks the IP addresses in these interactions to see if they belong to known subnets. IP addresses are verified for all IPv4 interactions. The application checks each interaction against Network Integrity Control rules (and registers the corresponding event if necessary) only if this interaction must be controlled according to the table below.

Subnets of IP addresses whose interactions are controlled

Source subnet	Destination subnet				
	Private, IT	Private, OT	Private, DMZ	Public	Link-local
Private, IT	no	yes	no	no	yes
Private, OT	yes	yes	yes	yes	yes
Private, DMZ	no	yes	no	no	yes
Public	no	yes	no	no	yes
Link-local	yes	yes	yes	yes	no

Example
When controlling interactions based on Network Integrity Control technology, the application checks all interactions in which the sources or destinations of network packets have IP addresses from **Private, OT** subnets. The application does not check interactions in which the destinations of network packets have IP addresses from **Private, DMZ** subnets while the network packet sources have IP addresses from **Private, IT** subnets.

Command Control technology is applied regardless of the specific subnet of the IP addresses of the sources and destinations of network packets containing system commands.

Interaction Control rules can be enabled or disabled.

By default, a rule is enabled after it is created and is applied to allow the described communications. The application does not register events when it detects interactions that are described in enabled rules.

Disabled rules are intended for describing unwanted network interactions. In learning mode for Interaction Control technologies, disabled rules prevent automatic creation of new enabled rules that describe the same network interactions. In monitoring mode, disabled rules are not taken into account.

The application processes Interaction Control rules based on Network Integrity Control and Command Control technologies if the use of these technologies is enabled. You can also configure the learning mode for these technologies.

The following methods are provided for creating a list of Interaction Control rules:

- Automatic generation of rules in learning mode.
- Manual creation of rules.

You can configure Interaction Control rules in the **Allow rules** section of the Kaspersky Industrial CyberSecurity for Networks web interface. This section contains a table with Interaction Control rules based on Network Integrity Control and Command Control technologies. This rules table may also contain allow rules created for events.

Events registered based on Network Integrity Control and Command Control technologies are categorized as system events.

You can view Interaction Control events in the table of registered events. Events registered based on Network Integrity Control technology have *High* severity. Events registered based on Command Control technology are assigned a severity that depends on the severity level defined for the detected system command.

Learning mode for Interaction Control technologies

In Interaction Control learning mode, the application does the following:

- If use of Network Integrity Control technology is enabled, the application generates rules based on this technology. Rules are generated for all IPv4 interactions that must be controlled according to the IP address subnet table for interaction control. When the application detects network interactions that match disabled rules, it registers events based on Network Integrity Control technology. The events are registered using the system event type that is assigned the code 4000002601.
- If the use of Command Control technology is enabled, the application generates rules based on this technology. When the application detects system commands that match disabled rules, it registers unauthorized system command detection events based on Command Control technology. The event is registered using the system event type that is assigned the code 4000002602.

When generating rules based on Interaction Control technologies, the application adds new rules obtained from its analysis of network interactions and system commands in industrial network traffic. For these rules, the **Origin** parameter contains the **System** value. If you manually change rule settings, the **Origin** parameter will take the **User** value.

Network interactions detected during traffic analysis are checked for compliance with current Interaction Control rules. If a detected interaction does not match any rule, the application creates a new rule. In this case, an interaction detection event is not registered. When a new rule is created, the application enables it and adds values of settings based on the received data about the network interaction.

If the detected interaction only matches a disabled rule, the application registers an event based on the technology corresponding to this rule. In this case, a new rule is not created.

During the learning process, the application can optimize the list of Interaction Control rules. Optimization involves combining two or more specific rules into one general rule, or deleting specific rules if a general rule is available. Rules that satisfy the following conditions are optimized:

- The rules are enabled.
- The **Origin** parameter contains the **System** value.
- The rules are related to the same technology.

Rules are merged during optimization if the resulting general rule will correspond only to the detected network interactions and no others. For example, one Interaction Control rule was created after a system command was detected during an interaction between two devices. Then another system command was detected during interaction between the same devices. In this case, after optimization, only one general rule will remain. It will describe both system commands detected during network interaction between these devices.

While operating in learning mode, the application periodically optimizes rules for the corresponding Interaction Control technology. The frequency of optimization is once per minute. Optimization is performed if new interactions are detected in industrial network traffic. To keep the rules table up to date, you must update rules.

After learning mode is disabled, optimization is performed one more time.

> There may be a delay before the Interaction Control rules are optimized after learning mode is disabled. The length of the delay depends on the amount of data being received by the application, and may last up to three minutes. During this time, it is recommended to refrain from making any changes to rules that were generated during learning mode based on Network Integrity Control and Command Control technologies.

Interaction Control learning mode must be enabled for enough time to receive all the necessary information about network interactions. This amount of time depends on the number of devices in the industrial network and how frequently they operate and are serviced. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period ranging from one to several days to accumulate the maximum amount of data.

Monitoring mode for Interaction Control technologies

In Interaction Control monitoring mode, the application does the following:

- If use of Network Integrity Control technology is enabled, the application checks devices' network interactions for compliance with the rules based on this technology. When the application detects network interactions for which there are no enabled rules, it registers unauthorized communication detection events based on Network Integrity Control technology. The events are registered using the system event type that is assigned the code 4000002601.
- If use of Command Control technology is enabled, the application checks devices' network interactions for compliance with the rules based on this technology. When the application detects system commands for which there are no enabled rules, it registers unauthorized system command detection events based on Command Control technology. The event is registered using the system event type that is assigned the code 4000002602.

Rules related to different technologies are applied independently of each other. Therefore, to allow use of a system command, the allow rules table must have rules created (automatically or manually) for this system command and for a network packet that transmits this command.

Automatic generation of Interaction Control rules in learning mode

In learning mode, Kaspersky Industrial CyberSecurity for Networks automatically generates Interaction Control rules. The application creates a new rule if the detected network interaction does not match any rule in the allow rules table.

When creating a rule, the application defines the values of parameters that are received from traffic pertaining to a detected network interaction.

If a Network Integrity Control rule is being created for an interaction in which the IP address of one of the sides of communication is in a subnet known to the application, the application might not add MAC addresses detected together with this IP address to the rule settings. Detected MAC addresses for IP addresses of a subnet are added if the **Ignore MAC addresses for NIC rules** toggle is switched off in the subnet settings.

In learning mode, the application can automatically create Interaction Control rules that allow transmission of system commands for Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes. These rules are needed for convenient joint use of applications within the integrated Kaspersky Industrial CyberSecurity solution. To automatically create rules prior to enabling learning mode, you must enable the PLC Project Integrity Check component on computers with Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes installed in this same industrial network. For detailed information on enabling this component, please refer to the Help System for Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes.

Viewing Interaction Control rules in the table of allow rules

Interaction Control rules are displayed in the allow rules table in the **Allow rules** section of the application web interface. Interaction Control rules include the following types:

- NIC rules based on Network Integrity Control technology.
- CC rules based on Command Control technology.

The settings of Interaction Control rules are displayed in the following columns of the table:

- **Rule ID**

  Unique ID of the rule.

- **Status** (icon ◐)

  Current status of the rule (*Enabled* or *Disabled*).

- **Rule type**

  For Interaction Control rules, this indicates the technology of the rule (NIC or CC). The EVT type is indicated for rules that disable event registration.

- **Protocols/Commands**

  For rules related to Network Integrity Control technology (NIC type) or rules that disable event registration (EVT type), this is the set of utilized protocols. For rules related to Command Control technology (CC type), this is the protocol and system commands. The protocols that are determined by the application based on the contents of network packets are italicized.

- **Side 1**

Device name/address information of one of the sides of network interaction. You can enable or disable the display of addresses and ports of address information by using the following settings: **MAC address**, **IP address**, **Port number**. If additional address spaces were added to the application, you can enable or disable the display of names of address spaces by using the following settings:

- **AS for MAC addresses** – address spaces containing the MAC addresses in the Interaction Control rule. This setting can contain the names of only those address spaces that have address space rules with the selected layer of the OSI model (**Data Link (L2)**).
- **AS for IP addresses** – address spaces containing the IP addresses in the Interaction Control rule. This setting can contain the names of only those address spaces that have address space rules with the selected layer of the OSI model (**Network (L3)**).

- **Side 2**

  Device name/address information of the other side of network interaction. The display of address information can be configured the same way as the **Side 1** column.

- **Comment**

  Additional information about the rule.

- **Created**

  The date and time when the rule was created.

- **Changed**

  The date and time when the rule was last modified.

- **Rule in event**

  The name of the Process Control rule or Intrusion Detection rule that must be indicated in the event (for EVT rules).

- **Monitoring point**

  The name of the monitoring point that must be indicated in the event (for EVT rules).

- **Event type**

  ID and title of the event type (for EVT rules).

- **Origin**

  Information about the origin of the rule.

When viewing the rules table, you can use the configuration, filter, search, and sorting functions.

Manually creating Interaction Control rules

You can manually create Interaction Control rules by doing the following:

- **Create a rule with initially empty values of settings or with the values from a template.**

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. In the **Allow rules** section, open the details area by clicking the **Add rule** button.

3. If you want to define the values of settings from a template, in the details area click the **Use template** button, select the necessary template in the opened window and click **Apply**.

4. In the details area, select the rule type corresponding to the relevant Interaction Control technology:

   - If you want to create a rule based on Network Integrity Control technology, click the **NIC** button.

   - If you want to create a rule based on Command Control technology, click the **CC** button.

5. In the **Protocol** field, specify the protocol for interaction between devices.

   When the **Protocol** field is selected, a window opens showing the table of supported protocols displayed as a protocol stack tree. You can manage how tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   If necessary, use the search field above the table to find relevant protocols.

   To specify the protocol:

   a. In the protocols table, select the protocol that you want to specify for the rule. To select the relevant protocol, click the button that is displayed in the left column of the protocols table.

      > For a Network Integrity Control rule, you can select any protocol that is displayed in the table of supported protocols. For a Command Control rule, you can select only a protocol from among the supported protocols for process control.

   b. Click **OK**.

   If you select a protocol that can be identified by the application based on the contents of network packets, a notification about this appears under the **Protocol** field.

6. If Command Control technology is selected for the rule, specify the relevant system commands in the **Commands** field.

   When the **Commands** field is selected, a window opens with a list of system commands that are available for the selected protocol. To specify the commands:

   a. In the list of system commands, select the check boxes next to the commands that should be allowed. If all commands should be allowed, you can either select all check boxes or clear all check boxes for all commands.

   b. Click **OK**.

7. If necessary, enter additional information about the rule in the **Comment** field.

8. In the **Side 1** and **Side 2** settings groups, specify the editable address information for the participants (sides) of network interaction. Depending on the selected protocol (or set of protocols), address information may contain a MAC address, IP address, and/or port number. If additional address spaces were added to the application, you can specify the names of the address spaces for addresses.

   To autofill the address information of a side of network interaction, you can select devices that are known to the application. To do so:

   a. Open the device selection window by clicking the **Specify device addresses** link.

   b. In the device selection window, select the check boxes next to the devices that you want to use.

      The device selection window contains a table in which you can configure the layout and order of columns, and filter, search, and sort similarly to the devices table in the **Assets** section.

   c. Click **OK** in the device selection window.

9. In the details area, click **Save**.

   The application checks the current list of Interaction Control rules.

10. If the Interaction Control rules include an enabled rule in which all the settings match, you will see a warning about the presence of a matching rule. In this case, close the warning and change the settings of the created rule.

11. If the Interaction Control rules include an enabled rule with more general settings, you will see a warning about the presence of a general rule. If a general rule is present, a new specific rule will not be used in the application. The warning will contain a prompt to save the new specific rule. To create a new rule with defined settings, confirm your decision in the prompt window (for example, if you want to then remove the general rule).

    The new rule will be added to the allow rules table.

12. If the Interaction Control rules include enabled rules with more specific settings, you will see a warning about the presence of more specific rules. After a general rule appears, the specific rules will not be used in the application. The warning will contain a prompt to remove the specific rules. To remove specific rules, confirm your decision in the prompt window.

    > If the rules table contains disabled rules with more specific or matching settings, the application removes these rules from the list. The application does not show a prompt when removing these rules.

13. If there is no enabled rule allowing network interaction between devices for a new rule based on Command Control technology, you will be prompted to create the corresponding rule based on Network Integrity Control technology. In this case, you are advised to create an additional rule together with the current rule being created. To do so, confirm your decision in the prompt window and perform the necessary actions to create a new rule based on Network Integrity Control technology.

- Create a new rule based on an existing rule. ?

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

  2. In the **Allow rules** section, select the rule that you want to use as the basis for creating a new rule.

  3. Right-click to open the context menu.

  4. In context menu select **Copy rule**.

     The details area in rule editing mode will appear in the right part of the web interface window. The settings of the new rule will take the values obtained from settings of the selected rule.

  5. Change the settings as necessary. To do so, complete steps 4–9 described in the procedure for creating a rule with initially empty values of settings.

- Create a rule based on an event registered for Network Integrity Control or Command Control technology.

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
  2. Select the **Events** section.
  3. In the table of registered events, select the event that you want to use as the basis for creating an Interaction Control rule.

     The details area appears in the right part of the web interface window.
  4. In the details area, click the **Create allow rule** button.

     The **Allow rules** section opens in the browser window. The details area in rule editing mode will appear in the right part of the web interface window. The new rule's settings will take the values received from the saved information about the event.
  5. If necessary, edit the settings of the new rule. To do so, complete steps 4–9 described in the procedure for creating a rule with initially empty values of settings. If you do not need to change the settings of the new rule, save the rule by clicking the **Save** button.

Editing Interaction Control rule settings

You can edit the settings of an enabled Interaction Control rule. You cannot edit disabled rules.

To edit the settings of an Interaction Control rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. In the **Allow rules** section, select the necessary NIC- or CC rule to edit its settings.

   The details area appears in the right part of the web interface window.
3. Click the **Edit** button.
4. Change the settings as necessary.

Enabling and disabling Interaction Control rules

Interaction Control rules can be assigned the *Enabled* status or the *Disabled* status. Rules are enabled by default after they are created.

You can disable rules that should not be used when Interaction Control technologies are operating in monitoring mode.

To change the status of the Interaction Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. In the **Allow rules** section, select the Interaction Control rules for which you want to change the status.

3. Enable or disable rules by using the **Enable** or **Disable** button. The buttons that are displayed depend on whether their corresponding operations are relevant for one or more of the selected rules.

   > If all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1,000, the application does not check the rule status. If this is the case, the details area displays both buttons for changing the state of rules.

Deleting Interaction Control rules

You can selectively delete one or multiple Interaction Control rules. Rules that are deleted are no longer applied for Interaction Control technologies, whether in monitoring mode or learning mode.

To delete Interaction Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Allow rules** section.

3. In the rules table, select the Interaction Control rules that you want to delete.

4. Click the **Delete** button.

   A window with a confirmation prompt opens. Depending on the state of the selected rules, the prompt will suggest the following options:

   - If all selected rules are enabled, the application prompts you to delete the selected rules, disable them, or cancel the operation. This condition is not checked if all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1,000.

   - If there are disabled rules among the selected rules or if all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1,000, the application prompts you to delete the selected rules or cancel the operation.

5. In the prompt window, confirm deletion of the rules.

Configuring Intrusion Detection

To detect intrusions in industrial network traffic, you can use Intrusion Detection rules and additional Intrusion Detection methods based on embedded algorithms. When signs of attacks are detected in traffic, Kaspersky Industrial CyberSecurity for Networks registers events based on Intrusion Detection technology.

Intrusion Detection methods and rules can be configured when connected to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. The list of Intrusion Detection rules is displayed in the **Intrusion Detection** section.

You can configure the settings for registering Intrusion Detection events under **Settings** → **Event types**.

You can view Intrusion Detection events in the table of registered events.

Intrusion Detection rules

An *Intrusion Detection rule* describes a traffic anomaly that could be a sign of an attack in the industrial network. The rules contain the conditions that the Intrusion Detection system uses to analyze traffic.

Intrusion Detection rules are stored on the Server and sensors.

The application applies intrusion detection rules when using the rule-based intrusion detection method. You can enable and disable this method.

Intrusion detection rules are grouped into sets of rules based on some attributes. For example, rules can be grouped by their purpose and included in a set designed to detect certain types of intrusions. You can use the following types of rule sets:

- System rule sets. These rule sets are provided by Kaspersky and are intended for detecting signs of the most frequently encountered attacks or unwanted network activity. System rule sets are available immediately after the application is installed. You can update system sets of rules by installing updates.
- User-defined rule sets. These rule sets are loaded into the application separately by the user. To load them, you need to use files containing data structures that define Intrusion Detection rules. These files must be in the same folder and have the RULES extension. The names of user-defined rule sets must match the names of the files from which these rule sets were loaded.

The application supports the application of no more than 50,000 rules cumulatively in all loaded rule sets. The limit on the number of loaded rule sets is 100.

> Rules loaded from user-defined rule sets may contain traffic analysis conditions whereby the application will register an excessive number of events when these rules are triggered. In this case, keep in mind that logging too many events may affect the performance of the Intrusion Detection System.

Sets of Intrusion Detection rules can be either enabled or disabled. Rules from the enabled set are applied during traffic analysis if the rule-based Intrusion Detection method is enabled. If a rule set is disabled, the rules from this rule set are not applied.

When a rule set is loaded, the application verifies the rules in the rule set. If errors are detected in the verified rules, the application blocks these rules from being applied. If errors are detected in all rules of the rule set or the rule set does not contain any rules, the application disables this rule set.

For information about sets of rules and detected errors, please refer to the **Intrusion Detection** section.

When the conditions defined in a rule from an enabled rule set are detected in traffic, the application registers a rule-triggering event. Events are registered with system event types that are assigned the following codes:

- 4000003000 – for an event when a rule from a system rule set is triggered.
- 4000003001 – for an event when a rule from a user-defined rule set is triggered.

User-defined rule sets may contain rules that were received from other Intrusion Prevention and Detection systems. When processing these rules, the application does not perform their defined actions that would otherwise be applied to network packets (for example, the `drop` and `reject` actions). When Intrusion Detection rules are triggered in Kaspersky Industrial CyberSecurity for Networks, only event registration is performed.

The scores of Kaspersky Industrial CyberSecurity for Networks events correspond to the specific priorities in Intrusion Detection rules (see the table below).

Mapping rule priorities to event scores

Intrusion Detection rule priority	Kaspersky Industrial CyberSecurity for Networks event score values
4 or higher	2.5
3	4.5
2	6.5
1	9

Additional Intrusion Detection methods

You can apply the following additional methods for Intrusion Detection:

- Detection of signs of falsified addresses in ARP packets (ARP spoofing) ?

  If detection of signs of falsified addresses in ARP packets is enabled, Kaspersky Industrial CyberSecurity for Networks scans the indicated addresses in ARP packets and detects signs of low-level man-in-the-middle (MITM) attacks. This type of attack in networks that use the ARP protocol is characterized by the presence of falsified ARP messages in traffic.

  When the application detects signs of falsified addresses in ARP packets, the application registers the events based on Intrusion Detection technology. Events are registered with system event types that are assigned the following codes:

  - 4000004001 – for detection of multiple ARP replies that are not associated with ARP requests.
  - 4000004002 – for detection of multiple ARP requests from the same MAC address to different destinations.

- TCP protocol anomaly detection ?

  If TCP protocol anomaly detection is enabled, Kaspersky Industrial CyberSecurity for Networks scans TCP segments of the data stream in supported application-level protocols.

  When it detects packets containing overlapping TCP segments with varying contents, the application registers an event based on Intrusion Detection technology. The events are registered using the system event type that is assigned the code 4000002701.

- IP protocol anomaly detection ?

> If IP protocol anomaly detection is enabled, Kaspersky Industrial CyberSecurity for Networks scans fragmented IP packets.
>
> When the application detects errors in the assembly of IP packets, it registers events for Intrusion Detection technology. Events are registered with system event types that are assigned the following codes:
>
> - 4000005100 for detection of a data conflict when assembling an IP packet (IP fragment overlapped).
> - 4000005101 for detection of an IP packet that exceeds the maximum permissible size (IP fragment overrun).
> - 4000005102 for detection of an IP packet whose initial fragment is smaller than expected (IP fragment too small).
> - 4000005103 for detection of mis-associated fragments of an IP packet.

- **Brute-force Attack and Scan Detection** ?

> If Brute-force Attack and Scan Detection is enabled, Kaspersky Industrial CyberSecurity for Networks analyzes network activity statistics to detect signs of brute-force attacks on account credentials, denial of service, scans, network service spoofing, and other anomalies.
>
> This method uses built-in rules. When rules are triggered, the application registers an event based on Intrusion Detection technology. The events are registered using the system event type that is assigned the code 4000003002.

You can enable and disable these methods. You can apply additional Intrusion Detection methods regardless of the availability and state of Intrusion Detection rules. Embedded algorithms are used for the additional scan methods.

Enabling and disabling sets of Intrusion Detection rules

Sets of Intrusion Detection rules can be assigned the *Enabled* status or the *Disabled* status. If a set of rules is disabled, no rules in this set are used for Intrusion Detection.

Whenever you enable or disable selected rule sets on all computers that have application components installed (Server and sensors), the Intrusion Detection system is restarted. A restart is required to apply the changes.

Only users with the Administrator role can change the states of sets of Intrusion Detection rules.

To change the status of Intrusion Detection rule sets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. In the **Intrusion Detection** section, select the sets of rules whose status you want to change.
3. Right-click to open the context menu.
4. In the context menu, select one of the following options:
    - **Enable** if you want to enable all disabled sets of rules from among the selected rule sets.

- **Disable** if you want to disable all enabled sets of rules from among the selected rule sets.
- **Change the statuses of selected rule sets** if you want to invert the statuses of all selected rule sets. This option lets you quickly enable or disable selected sets of rules with different statuses on all computers that have application components installed, as the Intrusion Detection System is restarted on all computers only once to apply all the changes together.

A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Loading and replacing user-defined sets of Intrusion Detection rules

You can load sets of Intrusion Detection rules from files into the application. Files containing descriptions of Intrusion Detection rules must be in the same folder and have the rules extension before you can load them into the application. The names of the files must not contain the following characters: `\ / : * ? , " < > |`.

After loading Intrusion Detection rules from a file, the rules are saved in the application as a user-defined rule set. The name of a rule set matches the name of the file from which this rule set was loaded.

> When sets of rules are loaded from files, the current user-defined rule sets are deleted from the table and replaced with the new ones. However, system sets of rules (whose **Origin** column shows the **System** value) are not deleted from the table.

Only users with the Administrator role can load user-defined sets of Intrusion Detection rules.

To load and replace user-defined sets of Intrusion Detection rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Intrusion Detection** section.
3. Click the **Replace all user-defined rules** link in the toolbar to open the window for selecting the folder containing Intrusion Detection rule files.
4. When the prompt window appears, click **OK**.
5. In the standard window of the browser you are using, select the folder containing the necessary files and click the button for transferring files from this folder.

   The table containing sets of rules displays the new user-defined sets of rules. For these sets of rules, the **Origin** column shows the **User** value. All sets of rules that have no detected errors will be enabled.
6. Check for errors in rules within the loaded sets of rules.

   Information about the detected errors is displayed in the **Rules** column. The *OK* status is displayed if there are no errors. If the set of rules contains errors, you can view detailed information about them by clicking the **Details** link.
7. If necessary, change the statuses of the rule sets (including the rule sets that have the *Errors in some rules* status).

Removing user-defined sets of Intrusion Detection rules

You can remove all user-defined sets of Intrusion Detection rules that were loaded into the application from files. You cannot selectively remove individual user-defined sets of rules. If you want to use only some of the existing rule sets in the application, you can copy files containing these rule sets into a separate folder and replace all user-defined rule sets with the rule sets from this folder.

Only users with the Administrator role can delete user-defined sets of Intrusion Detection rules.

To delete user-defined sets of Intrusion Detection rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Intrusion Detection** section.
3. Start deletion of user-defined rule sets by clicking the **Delete all user-defined rules** link in the toolbar.

   A window with a confirmation prompt opens.
4. In the prompt window, click **OK**.

All user-defined sets of Intrusion Detection rules will be deleted from the table.

Managing logs

This section contains information about managing logs of Kaspersky Industrial CyberSecurity for Networks.

Only users with the Administrator role can manage logs of Kaspersky Industrial CyberSecurity for Networks.

Managing the settings for storing logs in the Server database

You can change the settings for storing entries of logs in the Server database.

To change the settings for storing logs in the Server database:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the Server tile.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the Server parameters.
5. On the **General** tab, configure the following settings in the **Events**, **Audit entries**, and **Application messages** sections:

a. Use the **Max volume** setting to define the size limit for storing records. You can select the unit of measure for the defined value: **MB** or **GB**.

   When changing the value of this setting, please note the estimated maximum number of entries for the specified amount of space. You also need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

b. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for entries, and specify the minimum number of days to store them.

6. Click **Save**.

Managing the settings for saving traffic in the Server database

The application can save traffic received at the moment when events are registered. Traffic is saved in the Server database when registering events for which traffic saving is enabled. The application can also save traffic in the Server database directly by requesting to load traffic using temporary traffic dump files.

The application saves traffic data in blocks. If a traffic block relates to several events (when events are registered in a short time interval), this traffic block is not duplicated in the database.

To change the settings for saving traffic in the Server database:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Deployment**.

3. Select the Server tile.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

   The details area will show the tabs for configuring the Server parameters.

5. On the **General** tab, go to the **Traffic for events** group of settings, and use the **Max volume** setting to define the size limit for storing traffic.

   You can select the unit of measure for the space limit: **MB** or **GB**.

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

6. Click **Save**.

Managing the settings for saving traffic dump files

The application saves traffic received through the monitoring points as traffic dump files. These files are used by the application to analyze the incoming traffic. You can also use these files to perform the following actions in the application:

- Downloading traffic received by the node monitoring points

- Downloading traffic when working with the network interaction map

- Downloading network session traffic
- Downloading traffic for events (traffic dump files allow you to download traffic for events, even if traffic saving is disabled for the corresponding event types)

Traffic dump files are stored in the storages on the nodes where the application components are installed. On each node, both the internal storage of a node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used.

The application stores the traffic dump files temporarily. As traffic arrives, the application automatically deletes the oldest traffic dump files from the storages if the total volume of files approaches the limit set for the storage.

For each node, you can configure the settings for saving traffic to the internal storage. You can also connect the external storage of the node and configure the settings for saving traffic to the external storage.

To configure the settings for saving traffic dump files to the internal storage of the node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the tile of the relevant node.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the node parameters.
5. If necessary, on the **General** tab, in the **Filtering stored traffic** section, enable filtering and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

   > Filtering reduces the volume of the stored traffic by skipping the network packets that do not match the filter. However, when using filtering, keep in mind that the application may not receive all the data necessary for high-quality traffic analysis in the filtered traffic. Configure filtering so that all network packets that are required for traffic analysis according to the application functionality are saved in the traffic dump files.
6. Go to the **Traffic dump files** settings group and use the **Max volume** setting to define the size limit for storing traffic dump files.

   You can select the unit of measure for the space limit: **MB** or **GB**.

   When changing the value of this setting, you need to keep in mind that the volume and rate of incoming traffic and the sum of all space limits cannot exceed the defined maximum storage limit for the node.
7. Click **Save**.

Enabling and disabling the user activity audit

You can enable and disable the application user activity audit.

User activity audit is enabled by default.

To enable or disable the user activity audit:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Audit**.
3. Use the **User activity audit** toggle button in the toolbar to enable or disable the user activity audit.
4. Wait for the changes to be applied. The toggle switch is unavailable until it is finished moving to the other state.

Changing the logging level for processes

If application components are installed on nodes, these nodes have running processes that may save their operating data in logs in local folders. You can manage how data is saved in logs of the following application processes:

- On a computer that performs Server functions:
  - EntityManager
  - Filter
  - KisClient
  - NetworkDumper
  - ProductServer
  - Watchdog
  - WebServer
- On a computer that performs sensor functions:
  - EntityManager
  - Filter
  - NetworkDumper
  - Watchdog

For each process, you can assign one of the following logging levels:

- **Off**. Process data is not saved in the log.
- **Errors**. Data on process runtime errors is saved in the log.
- **Warning**. The log saves data from **Errors** and data requiring attention.
- **Info**. The log saves all data from the **Warning** logging level and reference information.

- **Debug**. The log saves all data covered under the **Info** logging level and all process data that may be required during the application debugging process (such as process performance data).

The logging levels may need to be changed, for example, when contacting Technical Support.

Only users with the Administrator role can change logging levels.

To change logging levels for Kaspersky Industrial CyberSecurity for Networks processes:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Logging**.
3. Change the logging levels as necessary:
   - To define the same logging level for all processes on all nodes, click the header of the column containing the name of the desired level.
   - To define the same logging level for all processes on one node, click a cell in the column containing the name of the desired level in the row containing the node name.
   - To define the log level for a process different from the logging levels defined for other processes, expand the list of processes of the relevant node in the **Nodes and processes** column and click a cell in the column containing the name of the necessary level in the row containing the process name.
4. Please wait for the changes to be applied (a progress indicator is displayed until the changes are fully applied).

Configuring operation with EPP applications

Kaspersky Industrial CyberSecurity for Networks can receive and process data received from Kaspersky applications that perform functions to protect workstations and servers. These applications are included in the Endpoint Protection Platform (EPP) and are installed to endpoint devices within the enterprise IT infrastructure.

Data transfer from EPP applications is performed by computers that have Kaspersky Endpoint Agent installed. Kaspersky Endpoint Agent is installed to workstations and servers in the enterprise IT infrastructure as a supplement to EPP applications.

Using the data received from EPP applications, Kaspersky Industrial CyberSecurity for Networks allows you to perform various actions on devices with Kaspersky Endpoint Agent installed.

The current version of Kaspersky Industrial CyberSecurity for Networks can receive and process data from the Kaspersky Endpoint Agent application included in the distribution kit of Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes. Kaspersky Endpoint Agent can be installed separately or as part of a specified application.

> If Kaspersky Endpoint Agent is installed on a device with an outdated operating system (for example, Windows 7), establishing the connection may fail. For information on how to fix the problems, contact Technical Support.

The maximum number of computers from which data from EPP applications can be received and processed is 1,000.

Data from Kaspersky Endpoint Agent is forwarded to Kaspersky Industrial CyberSecurity for Networks through *integration servers*. Integration server functions can be performed by any node that has a Kaspersky Industrial CyberSecurity for Networks component installed (Server or sensor). For integration with Kaspersky Endpoint Agent, you need to add integration servers to the nodes that will receive data from Kaspersky Endpoint Agent.

On a Kaspersky Industrial CyberSecurity for Networks node, integration server functions are implemented by the service named kics4net-epp-proxy that facilitates integration with EPP applications. The installation package for this service is included in the distribution kit of Kaspersky Industrial CyberSecurity for Networks.

When an integration server receives data from Kaspersky Endpoint Agent, the application may do the following:

- Register events based on EPP technology (workstation and server protection events).
- Populate the device table with devices hosting installed EPP applications (and devices that have had bidirectional interactions with such devices).
- Update the device table with information about devices hosting installed EPP applications (for example, the operating system version, information on the model or developer).
- Display special icons on the nodes of the network interactions map and the nodes of topology map, that indicate the presence and the connection status of EPP applications.
- Display on the map of network interactions the connections where one of the interaction parties is a device with an installed EPP application (in this case, data received from monitoring points traffic has priority when displaying information about such connections).
- Monitor the device equipment.
- Log network sessions.

When working with Kaspersky Endpoint Agent, you can perform the following actions using Kaspersky Industrial CyberSecurity for Networks:

- Use Kaspersky Endpoint Agent to scan devices as part of security audit jobs.
- Trigger response actions when logging events using the EPP technology, if threat development chains are built for these events in Kaspersky Endpoint Agent.

Computers hosting Kaspersky Endpoint Agent establish secure connections with integration servers over the HTTPS protocol. Connections are secured by using certificates issued by the Kaspersky Industrial CyberSecurity for Networks Server. The following certificates can be used in connections:

- Integration server certificate. This certificate is verified by the computer with Kaspersky Endpoint Agent each time a connection is being established. A connection is not established until certificate verification is successfully completed.
- Client certificate. This certificate is used to authenticate integration server clients that are computers with Kaspersky Endpoint Agent. The same client certificate can be used by multiple computers with Kaspersky Endpoint Agent. By default, an integration server does not verify certificates of clients, but you can enable client certificate verification to reinforce the security of connections.

Kaspersky Security Center is used to deliver certificates and public keys to computers with Kaspersky Endpoint Agent. This data is uploaded to Kaspersky Security Center using a communication data package, which needs to be created in Kaspersky Industrial CyberSecurity for Networks after an integration server is added.

Only users with the Administrator role can configure receipt of data from EPP applications.

Scenario for preparing to receive data from EPP applications

The scenario for preparing to receive data from EPP applications consists of the following phases:

1. **Installing EPP applications to computers of the monitored network**

   During this phase, you need to install Kaspersky applications that perform functions for protecting workstations and servers (EPP applications). EPP applications need to be installed on all computers whose data you want to receive in Kaspersky Industrial CyberSecurity for Networks. These computers must either reside outside of the industrial network (whose traffic is monitored through monitoring points) or have an additional connection to another network that includes one of the nodes that has a Kaspersky Industrial CyberSecurity for Networks component installed (for example, a connection to the Kaspersky Industrial CyberSecurity dedicated network). Kaspersky Endpoint Agent must be installed together with EPP applications.

   > In the current version, Kaspersky Industrial CyberSecurity for Networks supports receiving and processing data only when integrated with Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes. The versions of the specified applications that support operation in the integration mode are listed in the Hardware and software requirements article.

2. **Adding integration servers for nodes of Kaspersky Industrial CyberSecurity for Networks**

   This phase involves the completion of procedures for adding integration servers to nodes that computers with Kaspersky Endpoint Agent will connect to. Network interactions between nodes and these computers are possible only through network interfaces that are not being used as monitoring points. Specific network interfaces and IP addresses are not configured for integration servers because any available network interface and IP address of a computer can be used for an external connection to the integration server.

3. **Creating communication data packages for integration server clients**

   At this phase, you need to create and download communication data packages in which the application saves certificates and keys for connections between clients and integration servers. Each communication data package is an archive containing the following data:

   - Public certificate key of the integration server.
   - Certificate for integration server clients (with private key). This certificate is added if client certificate verification is enabled on the integration server. The certificate and key are saved in encrypted form with the password that was specified when the communication data package was created.

4. **Uploading integration server connection data to client computers**

   This phase is implemented by using the Kaspersky Security Center Administration Console and the Kaspersky Endpoint Agent administration plug-in. Computers with Kaspersky Endpoint Agent installed serve as clients for Kaspersky Industrial CyberSecurity for Networks integration servers. During this phase, you need to upload certificates and/or keys from communication data packages to the Kaspersky Security Center Administration Server by using the Kaspersky Endpoint Agent administration plug-in. Then, in the Kaspersky Security Center Administration Console, you need to create policies for uploading data to computers with Kaspersky Endpoint Agent. For information about working with data and creating policies, please refer to the Kaspersky Endpoint Agent documentation.

   For each integration server, you must create at least one policy containing the following data to be uploaded to the computers of clients:

   - Public certificate key of the integration server.
   - IP address for connecting to the integration server. You can indicate any of the available IP addresses of the node containing the integration server (you can view the IP addresses when connected to the Kaspersky

    Industrial CyberSecurity for Networks Server through the web interface on the **Integration servers** tab under **Settings** → **Connection Servers**). Port 8081 is the default port used for the connection.

    - Certificate for integration server clients (with private key). This certificate is added if client certificate verification is enabled on the integration server.

5. **Enabling integration servers**

   This phase is completed after applying policies and uploading data to computers with Kaspersky Endpoint Agent. During this phase, you need to enable all integration servers that will receive data from EPP applications. When an integration server is enabled on a node, the kics4net-epp-proxy service is activated.

When this scenario is fulfilled, Kaspersky Industrial CyberSecurity for Networks will begin to receive and process data from EPP applications.

Adding an integration server

To add an integration server:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Connection Servers**.

3. On the **Integration servers** tab, open the details area by clicking the **Add Kaspersky Endpoint Agent integration server** link.

4. In the **Node** drop-down list, select the node with the installed application component (Server or sensor) to which you need to add an integration server.

   You can only select a node that does not yet have an added integration server.

5. If necessary, enable verification of certificates for client authentication by using the **Verify client certificates** toggle switch.

6. If you enabled client certificate verification, create one or more certificates for integration server clients. To create a certificate, click the **Create new certificate** button. If necessary, you can remove unnecessary certificates from the list by using the 🗑 icon located on the right of the field containing the certificate fingerprint.

   If you created multiple client certificates, you can select the relevant certificate when creating the communication data package.

7. Click **Save**.

Creating a communication data package for integration server clients

After adding an integration server or changing its settings, you need to create and download a communication data package for clients of this server.

To create a new communication data package for integration server clients:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Connection Servers**.

3. On the **Integration servers** tab, select the server for whose clients you want to create a new communication data package.

   The details area appears in the right part of the web interface window.

4. Click the **Get communication data package for clients** button.

5. If client certificate verification is enabled for the integration server, the **Generating a new communication data package** window opens. Perform the following actions:

   a. In the **Certificate for clients** drop-down list, select the relevant certificate that will be used for authentication of integration server clients.

   b. Specify the password for accessing the selected certificate. Using the defined password, the certificate will be encrypted in the communication data package of the connector.

   c. Click the **Create communication data package** button.

The Kaspersky Industrial CyberSecurity for Networks Server generates a new communication data package for clients of the selected integration server, then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

You will need to upload the contents of the new communication data package to the computers of integration server clients. These uploads are performed by using Kaspersky Security Center Administration Server policies. In the Kaspersky Security Center policies, you need to specify the IP address for connecting to the integration server (to do so, you can use one of the available IP addresses indicated in the details area of the selected integration server).

Kaspersky Security Center policies are created and configured while configuring Kaspersky Endpoint Agent integration with Kaspersky Industrial CyberSecurity for Networks. For more information about configuring integration, please refer to the Kaspersky Endpoint Agent Help Guide.

Integration servers table

The integration servers table is displayed under **Settings** → **Connection Servers** on the **Integration servers** tab. This table displays information about integration servers that were added to nodes that have application components installed.

The integration servers table contains the following information:

- **Node name** – name of the node that has the application component installed.
- **IP addresses** – list of IP addresses on all network interfaces of the node (specific network interfaces and IP addresses are not configured for integration servers because any available network interface and IP address of a computer can be used for an external connection to the integration server).
- **Requests per second** – average number of successfully processed requests coming from clients to the integration server.
- **Status** – current status of the integration server.
- **Verify client certificate** – indicator of whether client certificate verification is enabled or disabled (if verification is disabled, the table cell is empty).

Enabling and disabling an integration server

Integration servers can be enabled or disabled. An integration server is disabled by default after it is created. Therefore, data from clients of this server is not processed in Kaspersky Industrial CyberSecurity for Networks.

To enable or disable an integration server:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection Servers**.
3. On the **Integration servers** tab, select the server that you want to enable or disable.

   The details area appears in the right part of the web interface window.
4. Click the **Enable** or **Disable** button.

Editing integration server settings

When editing integration server settings, you can replace the certificate for the integration server, and enable or disable client certificate verification and modify the list of certificates for clients.

To edit the integration server settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection Servers**.
3. On the **Integration servers** tab, select the server for whose clients you want to change the settings.

   The details area appears in the right part of the web interface window.
4. If you want to replace (issue a new) certificate for the same integration server, click the **Reissue certificate** button.

   After the integration server certificate is replaced, its old certificate becomes invalid.
5. If you want to enable or disable certificate verification for client authentication, use the **Verify client certificates** toggle switch.
6. If client certificate verification is enabled and you want to modify the list of certificates for clients, use the **Create new certificate** button and/or the 🗑 icon located on the right of the field containing the certificate fingerprint.
7. Click **Save**.

If a new certificate was issued for an integration server or if new client certificates were created, you need to once again create and download a communication data package to send data about these certificates to client computers.

Removing an integration server

To remove an integration server:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection Servers**.
3. On the **Integration servers** tab, select the server that you want to remove.

   The details area appears in the right part of the web interface window.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, click **OK**.

Managing response actions in Kaspersky Industrial CyberSecurity for Networks

If joint operation with EPP applications is configured in Kaspersky Industrial CyberSecurity for Networks, you can manually trigger the following response actions on devices:

- **Isolate device from the network**

  > After enabling network isolation of a device, Kaspersky Endpoint Agent terminates all active TCP/IP network connections on the device and blocks all new ones, except for the following connections:
  >
  > - Connections excluded from network isolation in Kaspersky Endpoint Agent.
  > - Connections initiated by services of the EPP application compatible with Kaspersky Endpoint Agent.
  > - Connections initiated by Kaspersky Endpoint Agent services.
  > - Connections initiated by Kaspersky Security Center Network Agent.
  >
  > Device network isolation remains active until network isolation is disabled in Kaspersky Industrial CyberSecurity for Networks. If network isolation is not manually disabled, it will be disabled automatically 9999 hours after it is enabled.

- **Prevent run**

  > You can configure rules to block the launch of executable files and scripts, as well as the opening of office format files on selected devices. For example, you can block the launch of applications that you consider unsafe on a selected device running Kaspersky Endpoint Agent. The application identifies files by their file path or checksum using the MD5 and SHA256 hashing algorithms.
  >
  > In the event of launch blocking, the user is notified about the triggered launch blocking rule. If the device user does not close the pop-up notification, it will close automatically 60 seconds after it appears.

- **Move to quarantine** ?

  > *Quarantine* is a designated local storage on a device running Kaspersky Endpoint Agent that stores files potentially infected with viruses or that were incurable at the time of detection. Quarantined files are stored encrypted and do not create a threat to the device security.
  >
  > By default, the local quarantine storage is located in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<version>\Quarantine folder. By default, objects restored from quarantine are stored in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<version>\Restore folder.
  >
  > Kaspersky Security Center generates a common list of quarantined objects on devices running Kaspersky Endpoint Agent. Device Network Agents transmit information on quarantined files to the Administration Server.
  >
  > Kaspersky Security Center does not copy quarantined files to the Administration Server. All objects are located on protected devices running Kaspersky Endpoint Agent. Objects are restored from quarantine on protected devices.

Response actions allow preventing or minimizing the consequences of detected threats from devices in an industrial network.

The capability to trigger response actions is available for devices with Kaspersky Endpoint Agent installed. When a response action is triggered, Kaspersky Industrial CyberSecurity for Networks transmits the information about it to Kaspersky Endpoint Agent installed on the device. Kaspersky Endpoint Agent executes the received command and sends a completion notification to Kaspersky Industrial CyberSecurity for Networks.

Once the triggered response action is completed and the threat from the device is eliminated, you can trigger the corresponding reverse action. For the listed response actions, the following reverse actions are available:

- **Disable network isolation**.
- **Disable run prevention**.
- **Restore from quarantine**.

Kaspersky Industrial CyberSecurity for Networks registers triggered response actions and the corresponding reverse actions. The registered actions are displayed in the **Events** section on the **Response actions** tab.

You can trigger response actions by selecting the relevant events, devices or previous response actions that were registered and completed. The actions available to you depend on the selected object. For example, if you selected a device with Kaspersky Endpoint Agent installed, you only can manage the network isolation for this device. Other response actions (**Prevent run** and **Move to quarantine**) are available when selecting the event associated with this device and if a threat development chain is built for the event in Kaspersky Endpoint Agent.

Only the users with the Administrator role can trigger response actions and corresponding reverse actions.

Triggering event response actions

You can trigger response actions on a device using a registered event that is associated with such device. To trigger a response action, an event must be associated with a device with Kaspersky Endpoint Agent prepared according to the scenario for preparing to receive data from EPP applications.

When working with events, you can trigger the following response actions:

- **Isolate device from the network** — for any event associated with a device with Kaspersky Endpoint Agent installed.
- **Prevent run**, **Move to quarantine** — for an event based on EPP technology if a threat development chain is built for this event in Kaspersky Endpoint Agent and includes an activity event with a threat detection object and the **File creation** or **Starting a process** type. You can also trigger the **Isolate device from the network** action for such events.

For events that are EDR incidents, you can trigger the **Prevent run** and **Move to quarantine** actions both for the threat detection object and for objects specified in other activity events with the **File creation** or **Starting a process** type.

To isolate a device associated with an event from the network:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the event on the **Events and incidents** tab in the **Events** section.

   You can select an EDR incident or any event associated with the device with Kaspersky Endpoint Agent installed.

   The details area appears in the right part of the web interface window.
3. In the details area, open the **Threat response** drop-down list and select **Isolate device from the network**.

   A window with a confirmation prompt opens.
4. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

To prevent execution or move to quarantine a threat detection object:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the event on the **Events and incidents** tab in the **Events** section.

   You can select an EDR incident if the threat development chain includes an activity event with a threat detection object and the **File creation** or **Starting a process** type.

   The details area appears in the right part of the web interface window.
3. In the details area, open the **Threat response** drop-down list and select the appropriate item:
   - **Prevent run** — if you want to prevent the threat detection object from execution.
   - **Move to quarantine** — if you want to move the threat detection object to quarantine.

   A window with a confirmation prompt opens.
4. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

*To prevent execution or move to quarantine an object specified in any activity event with the **File creation** or **Starting a process** type in the threat development chain:*

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the event on the **Events and incidents** tab in the **Events** section.

   You can select an EDR incident.

   The details area appears in the right part of the web interface window.

3. In the details area, go to the **All activity events** tab and select the appropriate activity event.

   You can select any activity event with the **File creation** or **Starting a process** type. A key activity event (with a threat detection object) is marked with the **Detection** icon.

4. In the activity event details window that opens, click the appropriate button:

   - **Prevent run** — if you want to prevent the object from the selected activity event from execution.

   - **Move to quarantine** — if you want to move the object from the selected activity event to quarantine.

   A window with a confirmation prompt opens.

5. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering device response actions

You can trigger the Isolate device from the network **response action** and its corresponding reverse action **Disable network isolation** on a device. To manage network isolation, the device must run Kaspersky Endpoint Agent prepared according to the scenario for preparing to receive data from EPP applications.

To trigger a response action for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device on both the network interactions map and the topology map.

   The details area appears in the right part of the web interface window.

3. In the details area, open the **Threat response** drop-down list and select the appropriate item:

   - **Isolate device from the network** — if you want to isolate the selected device from the network.

   - **Disable network isolation** — if you want to disable network isolation of a device for which the **Isolate device from the network** action was previously triggered.

   Items in the **Threat response** drop-down list are available if Kaspersky Endpoint Agent is installed on the device.

   A window with a confirmation prompt opens.

4. In the request window, confirm the start of the response action.

   The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering response actions when working with registered response actions

If a response action is triggered in Kaspersky Industrial CyberSecurity for Networks (when working with events or devices), you can trigger the corresponding reverse action on the **Response actions** tab of the **Events** section. For example, if the **Isolate device from the network** action is triggered for a device, you can trigger the **Disable network isolation** action for this device when working with registered actions.

After registering a reverse action, you can use it to trigger the next response action for the same device or object. For example, if you want to isolate a device from the network again after disabling the network isolation.

For the **Disable run prevention** and **Restore from quarantine** registered actions, you can trigger both **Prevent run** and **Move to quarantine** as a reverse action.

To trigger a response action that is reverse in respect of a registered action:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the action on the **Response actions** tab in the **Events** section.

   The details area appears in the right part of the web interface window.
3. In the details area, click the reverse action start button. For example, if you selected the **Isolate device from the network** action, click the **Disable network isolation** button to trigger the reverse action.

   A window with a confirmation prompt opens.
4. In the request window, confirm the start of the response action.

   The application will register a new response action.

Viewing the response action table

The response actions table is displayed on the **Response actions** tab in the **Events** section. The table shows the response actions that are registered when the response actions are triggered in Kaspersky Industrial CyberSecurity for Networks.

Response action settings are displayed in the following columns of the table:

- **ID**

  Unique ID of the registered action.
- **Start**

  Action start date and time.
- **End**

  The date and time when the action was completed or a confirmation of the action was received. If the application has not received a confirmation of the action, the date and time when the time-out period expires for the action to be performed is displayed.

- **Action type**

  The type of the registered action. The following types are provided:

  - **Isolate device from the network**.
  - **Prevent run**.
  - **Move to quarantine**.
  - **Disable network isolation**.
  - **Disable run prevention**.
  - **Restore from quarantine**.

- **Status**

  Action completion status. The following statuses are available:

  - *Pending* — a command to start the action has not been sent yet.
  - *In progress* — the action is being started or is in progress.
  - *Success* — the action is completed successfully.
  - *Failure* — an error occurred when performing the action or the action was canceled due to expiry of the period for receiving a confirmation.

- **Device**

  The name of the device for which the action was triggered.

- **Event title**

  The event title if the action was triggered while working with the event.

- **Object type**

  The type of an object for which the action was triggered.

- **Object**

  The name of the object for which the action was triggered.

When viewing the response action table, you can use configuration, filter, search and sort functions, and navigate to the related items.

Deleting response actions

You can delete registered response actions. However, you cannot delete actions with the *In progress* status.

> Before deleting a response action, the application checks the current status of this action. However, during and after deletion of an action, the application does not monitor the operations for this action performed on the device and does not cancel operations if they have already started. As a result, a response action may be performed on the device even if this action had the *Pending* status at the time of deletion.

Deleting a registered action does not override the result of the action performed on the device. For example, if a successfully completed **Isolate device from the network** action is deleted, network isolation of the device continues after the action is deleted. To disable network isolation, the **Disable network isolation** action must be triggered.

To delete a response action:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the action on the **Response actions** tab in the **Events** section.
3. Click the **Delete action** button.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm the deletion of the action.

Managing connectors

This section contains information about managing connectors in Kaspersky Industrial CyberSecurity for Networks. *Connectors* are specialized application modules that facilitate the exchange of data with Kaspersky Industrial CyberSecurity for Networks and may provide capabilities to perform management tasks in the application directly or through use of the application.

Connectors expand application functionality for interaction with recipient systems, including with Kaspersky Security Center. Depending on their functional purpose, connectors can transmit data to recipient systems (for example, relay events, application messages and audit entries to a SIEM system) or receive data from recipient systems (for example, to register External events in the application). The application may also use connectors to conduct active polling of devices.

A specialized connector named **Kaspersky Security Center Connector** is used so that the application can interact with Kaspersky Security Center. This connector is created in the application by default and cannot be deleted. To ensure proper functioning of the connector, the capability for the application to interact with Kaspersky Security Center must be added to the Kaspersky Industrial CyberSecurity for Networks Server.

Computers running application modules of connectors are called *connector deployment nodes*. A connector deployment node can be any computer that has network access to the application Server computer (such as nodes that have application components installed, including the actual computer of the Server).

The functional capabilities of the connector depend on the selected *connector type*. You can select the relevant connector type when adding a connector to the application. The application has the following built-in connector types by default:

- **Syslog** – provides the capabilities for forwarding data to a Syslog server.
- **SIEM** – provides the capabilities for forwarding data to the server of a SIEM system.
- **Generic** – provides the capabilities for connecting applications that utilize the Kaspersky Industrial CyberSecurity for Networks API.
- **Email** – provides the capabilities for forwarding data in email messages.
- **Active poll** – provides the capabilities for active polling of devices.

- **KUMA**—if there are installed software modules, provides the capabilities of integration with Kaspersky Unified Monitoring and Analysis Platform (hereinafter also KUMA). Software modules for this type of connectors are supplied separately from Kaspersky Industrial CyberSecurity for Networks. Using this type of connector, you can send information about devices and risks to KUMA, as well as use the commands to change device statuses in KUMA. After adding the connector, configure the integration in KUMA (create a connection to Kaspersky Industrial CyberSecurity for Networks). Interaction between the KUMA connector and the Server is performed using the Kaspersky Industrial CyberSecurity for Networks API.

  > The KUMA connector provides integration by sending information about devices and risks and applying commands to change device statuses. To send events to KUMA, add a **Syslog** or **SIEM** connector to Kaspersky Industrial CyberSecurity for Networks and specify the data for connecting to the KUMA server for this connector. After adding a connector, configure the collector on the KUMA side.

If necessary, you can add other types of connectors that will facilitate data exchange or provide the capabilities for performing management tasks when the application interacts with other recipient systems.

Certain ports and protocols are used to connect the connectors to the Server.

A recipient system is connected through a connector on behalf of one of the application users. It is recommended to use a separate user account for each connector. This will make it more convenient to analyze the actions that are performed through connectors based on audit entries.

The connectors table and connector types table are displayed under **Settings** → **Connectors** in the application web interface. Only users with the Administrator role can manage connectors and connector types.

Maximum number of connectors in the application – 20. Maximum number of connector types – 100.

About manageable and unmanageable connectors

Manageable and unmanageable connectors can be used in the application.

A connector is *manageable* if its application modules can access functions for automatic registration and startup after the connector is added, and can access functions for managing these modules when enabling or disabling the connector or when deleting it. Only nodes that have application components installed can serve as deployment nodes for manageable connectors.

An *unmanageable connector* does not provide the functions of a manageable connector. Registration of this type of connector, and startup, stoppage, and deletion of its application modules must be performed manually on the connector deployment node. When an unmanageable connector is enabled or disabled, interaction with this connector on the Server side is allowed or blocked, respectively.

The connections between connectors and the application Server are secured by using certificates. Certificates are created for connectors when these connectors are added to the application. The application automatically forwards the created certificates for application modules of manageable connectors. When adding an unmanageable connector (or when adding a manageable connector configured to ignore the functions of a manageable connector), the certificate for application modules of this connector must be manually uploaded using a communication data package. If you need to replace (issue a new) certificate for this type connector, you must create a new communication data package and use this file to upload the new certificate. Certificates of manageable connectors can be replaced only by deleting these connectors and then adding them again.

About forwarding events, application messages and audit entries to recipient systems

You can configure forwarding of events, application messages, or audit entries (hereinafter also referred to as "registered notifications") to a recipient system by using connectors. For the types of connectors named **Syslog**, **SIEM**, **Email**, and **Kaspersky Security Center Connector**, the capability to forward registered notifications is enabled by default. For the **KUMA** connector type, the capability to forward registered notifications is available if application modules are installed. When using other types of connectors that were added to the application, this capability is available depending on the settings defined for these specific connector types.

The settings for forwarding registered notifications are configured for each connector individually. When configuring event types, you can select the relevant event types to forward via connectors. When creating a connector or changing its settings, you can enable or disable forwarding of all application messages and all audit entries through this connector.

Some types of connectors provide the capability to limit the volume of transmitted data. This limit is applied for a 24-hour period starting at 0:00 in the time zone of the Server. You can set a limit on the volume of transmitted data for the following system types of connectors:

- **Email**. For this type of connector, you can define the maximum number of email messages regarding new registered notifications and the maximum number of registered notifications in each message. If the maximum number of email messages has been sent, message recipients receive one more message notifying them that the maximum number has been exceeded. After this, new messages will not be sent until the end of the current day.
- **Kaspersky Security Center Connector**. For this type of connector, you can define the maximum number of registered notifications that can be forwarded. If the number of registered notifications exceeds this maximum number, the excess notifications registered before the end of the current day are not sent to Kaspersky Security Center.

> Events containing information about multiple network interactions are specially forwarded as follows. Each of these events is considered as one item when forwarded through the **Kaspersky Security Center Connector**. However, when it is being forwarded, the event is converted into multiple registered notifications, with each notification representing one network interaction. For this reason, the list of registered notifications for the **Kaspersky Security Center Connector** may contain more notifications than defined by the setting that determines the maximum number of notifications.

The contents and order of information about registered notifications forwarded through **Syslog** and **SIEM** connectors may differ from the contents and order of information displayed on pages of the Kaspersky Industrial CyberSecurity for Networks web interface.

Email messages forwarded through an **Email** connector are generated separately for each type of registered notification. In other words, separate email messages are generated to forward events, application messages, and audit entries.

Adding a connector

You can add a connector based on one of the connector types that are available in the application.

To use all KUMA integration capabilities, add two types of connectors. To send information about devices and risks to KUMA and use the commands to change device statuses, add a **KUMA** connector. To send Kaspersky Industrial CyberSecurity for Networks events to KUMA, add a **Syslog** or **SIEM** connector and specify the data for connecting to the KUMA server for this connector.

Prior to adding a connector, you are advised to create a separate user account that the recipient system will use to connect to the application.

To add a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, open the details area by clicking the **Add connector** link.
4. Select the relevant connector type and enter the connector name.
5. If you want to add an unmanageable connector (or a connector configured to ignore the functions of a manageable connector), enter the password for accessing the connector certificate.

   Using the defined password, the certificate will be encrypted in the communication data package of the connector.
6. Specify the address of the application Server.

   The connector will connect to the Server at the specified address.
7. Specify the connector deployment node:
   - If you want to add a manageable connector, you can use one of the nodes that have application components installed as the connector deployment node.
   - If you want to add an unmanageable connector, you need to enter the IP address of the computer where the connector application modules will be running.
8. Select the user account that the recipient system will use to connect to the application through the connector. You must indicate the name of one of the application users.
9. In the **Details** block, specify the advanced settings depending on the type of connector. The **Details** block is not shown in the details area if the connector type does not allow configuration of advanced settings.

   For connector types that are built into the application by default, you can configure the following settings:
   - **SIEM** / **Syslog**:
     - Server address.
     - Server port.
     - Data Transfer Systems.
   - **Email**:
     - Address indicated as the sender of email messages.

  - Recipient addresses of email messages.
  - Subjects of email messages for events, application messages, and audit entries.
  - Templates of text descriptions for events, application messages, audit entries, network interactions, and for entire messages containing notifications. Templates are formed by using variables.
  - Subject and text of an email message notifying when the maximum number of sent notifications is reached.
  - Maximum number of email messages sent per day.
  - Maximum number of notifications in each message. Defines the maximum number of registered notifications of one type (events, application messages, or audit entries) that can be put into one email message. If the number of registered notifications exceeds the maximum number, an additional email message is generated (within the daily limit).
- **Active poll**:
  - Active polling methods that will be available to the application user when using the connector.
  - The ranges of allowed and denied IP addresses of the devices for which active polls are allowed or denied. The address `0.0.0.0` corresponds to all possible IP addresses. If an address is included in the range of both allowed and denied IP addresses, Kaspersky Industrial CyberSecurity for Networks treats it as a denied IP address.
  - Names of address spaces whose corresponding devices will be available for active polling. If necessary, select the address spaces for IP addresses in the **L3 address space** field and select the address spaces for MAC addresses in the **L2 address space** field.

10. If the connector type provides the capability to forward application messages and audit entries, use the corresponding check boxes to enable or disable forwarding of this data.
11. Enter a connector description if necessary.
12. Click **Save**.

    The new connector will appear in the connectors table.

    If an unmanageable connector was added, the Server generates a communication data package for the new connector. Then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file. You will need to upload the contents of the new communication data package to the app that will use the connector.
13. For an unmanageable connector, create a service on the node hosting the connector. To do so, you can use the corresponding script:
    - If a **Syslog**, **SIEM**, **Generic**, or **Email** connector has been added, you can create a service by using the default_connectors_registrar.py script located in the directory /opt/kaspersky/kics4net-connectors/libexec/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

      ```
      sudo python3 default_connectors_registrar.py create
      ```

      When prompted by the script to provide connector data, enter the name of the connector, the path to the communication data package, and the connector certificate access password.
    - If an **Active poll** connector has been added, you can create a service by using the register.py script located in the directory /opt/kaspersky/kics4net-apm/src/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

```
sudo python3 register.py -p "<full path to the communication data package>"
```

Viewing the connectors table

The connectors table is displayed on the **Connectors** tab in the **Settings** → **Connectors** section.

The connector settings are displayed in the following columns of the table:

- **Name**.

  Defined name of the connector.

- **Connector ID**.

  ID assigned to the connector when it was created.

- **Enabled**.

  Indicates whether the Server is ready for interaction with application modules of the connector. If this setting has the **No** value, the Server does not accept requests from application modules of the connector.

- **Status**

  Operating status of application modules of the connector. The following statuses are available:

  - *Awaiting registration* – after adding an unmanageable connector or after creating a new communication data package for the unmanageable connector, no connection has been established through this connector.

  - *Switchover* – the operating status of application modules of the connector is switched from *Not running* status to *Running* status, or vice versa.

  - *Not running* – the Server does not accept requests from application modules of the connector. If the connector is manageable, the command to stop running is sent to its application modules.

  - *Running* – a successful connection was established through this connector using the certificate created for this connector.

  - *Error* – an error occurred when attempting to perform actions with the application modules of the connector.

- **Type**.

  Icon and name of the connector type.

- **Last connection**.

  Date and time of the last connection through this connector.

- **Manageable**.

  Indicates that the connector is manageable. If this setting has the **No** value, the connector is either unmanageable or is configured to ignore the functions of a manageable connector.

- **Changed**.

  Date and time of the last modification of the connector settings.

- **Description**

  Defined description of the connector.

When viewing the connectors table, you can use the configuration, filter, search, and sorting functions.

Enabling and disabling a connector

If you want to temporarily prevent the application modules of a connector from connecting to the Server, you can disable this connector. To resume the connection, you will have to enable the connector.

To enable or disable a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the connector that you want to enable or disable.

   The details area appears in the right part of the web interface window.
4. Click the relevant button: **Enable** or **Disable**.

   A window with a confirmation prompt opens.
5. In the prompt window, click **OK**.

Editing connector settings

To edit connector settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the relevant connector.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.
5. You can edit the settings the same as when you added the connector.

   Not all settings are available for editing. For example, the selected connector type cannot be changed.
6. Click **Save**.

   The changes will be displayed in the corresponding columns of the connectors table. If you changed the connector name, the new name is displayed in the column header in the event types table.

When certain settings of an unmanageable connector are changed, the Server will generate a new communication data package for the connector (for example, this occurs if you change the server address for a **Syslog** connector that is configured to ignore the functions of a manageable connector). Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved communication data package. You will need to upload the contents of the new communication data package to the application that uses the connector. Otherwise, a new connection through the connector will be impossible for this app.

Creating a new communication data package for a connector

When an unmanageable connector is added, a communication data package is automatically created for this connector. If necessary, you can create a new communication data package for a connector (for example, if the certificate from the previous communication data package has been compromised).

After a new communication data package is created, the certificate from the old communication data package becomes invalid. For this reason, you will have to use the new communication data package the next time you connect a recipient system through this connector.

To create a new communication data package for an unmanageable connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the unmanageable connector for which you want to create a new communication data package.

   The details area appears in the right part of the web interface window.
4. Click the **Get new communication data package** button.

   The **Generating a new communication data package** window opens.
5. Specify the settings for generating the communication data package:
   - User name that the recipient system will use to connect to the application through the connector. You must indicate the name of one of the application users.

     It is recommended to specify the user name that was indicated when adding the connector. If you need to specify the name of a different user, you are advised to select an application user account that was not indicated for other connectors and is not being used to connect to the Server through the web interface.
   - Address of the node where the connector application modules are running.
   - Password for accessing the connector certificate. Using the defined password, the certificate will be encrypted in the communication data package of the connector.
6. Click the **Create communication data package** button.

The Server generates a new communication data package for the selected connector, then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file. You will need to upload the contents of the obtained communication data package to the application that uses the connector. Otherwise, a new connection through the connector will be impossible for this app.

Deleting a connector

When a manageable connector is deleted, its application modules are automatically stopped and deleted from the connector deployment node.

Prior to deleting an unmanageable connector (or a connector that is configured to ignore the functions of a manageable connector), you first need to stop it manually and delete its application modules.

To prepare an unmanageable connector for deletion:

On the node where the connector is deployed, perform one of the following actions as appropriate:

- For a **Syslog**, **SIEM**, **Generic**, or **Email** connector, use the default_connectors_registrar.py script located in the directory /opt/kaspersky/kics4net-connectors/libexec/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

  ```
  sudo python3 default_connectors_registrar.py delete
  ```

  After starting the script, specify the name of the connector when prompted by the script.

- For an **Active poll** connector, enter the following command in the operating system console:

  ```
  sudo systemctl disable kics4net-apm
  ```

To delete a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Connectors**.

3. On the **Connectors** tab, select the connector that you want to delete.

   The details area appears in the right part of the web interface window.

4. Click the **Delete** button.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm removal of the selected connector.

Adding and deleting connector types

Connector types determine the available functional capabilities of connectors and the specific functionality that can be implemented within the scope of those capabilities. You can use the connector types that are already built into the application by Kaspersky and you can use additional connector types from other vendors.

To add a connector type to the application, you must obtain the following files from the vendor:

- Files for installing the application modules of connectors

- Connector type description file

> If a connector type from a third-party vendor lets you save user account credentials in connectors for access to a recipient system, it is recommended to take measures to prevent these account credentials from being compromised. To minimize risks in case account credentials are compromised, it is recommended to provide only the minimum required permissions that these user accounts need for connections through the connectors.

The files for built-in connector types are included in the application distribution kit. These files are used to add connector types automatically during installation of application components. If built-in connector types are removed from the application for some reason, you can use the files from the distribution kit to re-add these connector types.

The connector types table is displayed under **Settings** → **Connectors** on the **Connector types** tab.

Viewing the connector types table

The connector types table is displayed under **Settings** → **Connectors** on the **Connector types** tab.

The connector settings are displayed in the following columns of the table:

- **Name**

  Connector type name defined by the vendor.

- **Vendor**.

  Name of the connector type vendor.

- **Version**.

  Connector type version number.

- **Code**.

  Unique number of the connector type.

- **Capabilities**.

  List of functional capabilities that will be available for connectors of this type.

When viewing the connector types table, you can use the configuration, filter, search, and sorting functions.

Adding a connector type

You can add a connector type to the application by using the description file provided by the vendor of this connector type. The description file of a connector type must be in a ZIP archive.

Installation of application modules for connectors of an added connector type must be performed manually using the files provided by the vendor of the connector type. Application modules need to be installed on the computers that will be specified as the connector deployment nodes when adding connectors.

To add a connector type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Connectors**.

3. On the **Connector types** tab, open the details area by clicking the **Add connector type** link.

4. Use the **Browse** button to select the connector type description file.

5. Click **Save**.

The new connector type will appear in the connectors table.

Deleting a connector type

When a connector type is deleted from the application, the application also deletes the information about this connector type as well as all connectors that were added using this connector type.

To delete a connector type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connector types** tab, select the connector type that you want to delete.

   The details area appears in the right part of the web interface window.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm removal of the selected connector type.
6. If the application has connectors of this type, also confirm removal of these connectors.

Performing active polling of devices

When working with Kaspersky Industrial CyberSecurity for Networks, you can conduct *active polling of devices* to receive the most accurate and complete information about devices and their configurations directly from the devices. Active polls are performed by using connectors. To conduct active polling of devices, one or more **Active poll** connectors must be added to the application.

Connectors provide various methods for conducting active polling. The available *active polling methods* depend on the utilized protocols and the commands and functions of these protocols. The application's built-in **Active poll** connector type contains a set of methods that support active polls over application-layer protocols and common protocols. Kaspersky Industrial CyberSecurity for Networks supports the following methods to actively poll the devices:

- Receiving information about the operating system via the SMB protocol.
- Receiving information about the device via the Beckhoff (UDP) protocol.
- Receiving information about the device via the CIP™ (EthernetIP) protocol.
- Receiving information about the device via the DNP3 protocol.
- Receiving information about the device via the MMS protocol.
- Receiving information about the device via the modbus protocol.
- Receiving information about the device via the s7comm (Ethernet) protocol.
- Receiving information about the device via the s7comm (TCP) protocol.

- Receiving information about the device via the SNMP v1, v2c, v3 protocol.

- Receiving general information about the device via SSH.

- Receiving general information about the device via WInRM (HTTP).

- Receiving general information about the device via WInRM (HTTPS).

- Receiving general information about the device via WMI.

- Receiving information about the device vendor by MAC address via ARP (only for the computers with kernel version 4.3 and later).

- Receiving information about the device via the Profinet-DCP protocol (only for the computers with kernel version 4.3 and higher).

- Scanning an industrial configuration and getting a list of tags (only for the computers with kernel version 4.3 and higher).

The methods are distinguished by the specific device information that they obtain. You can select the relevant information you need and the methods you want to use when configuring the active polling settings.

When using these methods, the application can automatically update the following device information based on the active polling results:

- Name used to represent a device in the application.

- Name used to represent the device in the network (network name).

- Name of the device hardware vendor.

- Device model name.

- Device hardware version number.

- Name of the device software vendor.

- Device software name.

- Device software version number.

- Address information for network interfaces of the device.

- Name of the operating system installed on the device (only for devices running Windows and Linux operating systems).

- Configuration of Process Control settings and tags.

The list of operating systems supported by the application for active polling of devices is provided in the Appendix.

The application does not update data for which the automatic update function was disabled using the **Auto update** toggle button when the device was added or when device information was edited. The application also evaluates the authenticity of received device information and in some cases may reject unreliable updates of previously received information.

Some active polling methods support the capability to detect risks and to make changes to the topology map based on obtained device information.

Only users with the Administrator role can run active polling of devices.

To utilize active polling functionality, you need to take into account the following special considerations and limitations:

- This functionality is available after a license key is added.
- Application modules of the connectors used to conduct active polling of devices must have network access to the devices so that they can send requests and receive data from the devices. If application modules are running on a node that has application components installed, to ensure network access to devices this computer must have a network interface with a connection to the network of these devices. Network interfaces of monitoring points cannot be used for this purpose if these network interfaces receive mirrored industrial network traffic (for example, from SPAN ports of network switches).
- Active polling may result in some unforeseen issues with devices due to the possibility that these devices may incorrectly interpret the incoming active polling commands. These issues may be caused by an inappropriate or highly specialized configuration of devices. Issues may also arise due to latent errors in the network configuration that are not apparent during normal interactions between the devices. Consequently, active polling poses the following risks of potential impact on devices:
  - Device shutdown
  - Loss of connectivity with the device
  - Impaired performance of the device
  - Other potential malfunctions in the network and equipment

Configuring and starting active polling

You can configure and run active polling for one device or simultaneously for multiple devices from the devices table.

The ability to run active polls is available after adding a license key.

Active polling is configured and started by using a wizard. The Active Polling Configuration Wizard automatically determines the available active polling methods depending on the selected devices and the selected settings that you need to receive. Active polling is started at the final step of the wizard.

The active polling configuration wizard can be invoked in the following ways:

- **Invoking the wizard when working with the devices table**

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to run active polling. You can select no more than 16 devices when configuring and running active polling.

4. In the toolbar above the devices table, open the **Perform** drop-down list and select **Active polling**.

   The active polling configuration wizard window opens.

5. If no application user has previously conducted active polling of devices, the wizard window will show a warning regarding the specifics of active polling. Carefully read the warning and confirm that you accept the risks of potential impacts when using the active polling module.

6. In the **Select parameters** section of the wizard, select the check boxes for the specific device information that you want to update using active polling. You can also enable risk detection (the **Risks** check box) and discovery of topology settings for devices (the **Topology settings** check box).

7. In the **Select polling methods** section of the wizard, select the check boxes for the specific methods that you want to use for getting device information, risk detection, and/or reading topology settings.

   The available methods are grouped based on the connectors that provide the capabilities for active polling of devices. The list contains only the methods that are capable of obtaining the selected information. If a connector cannot be used for active polling of selected devices, available methods are not displayed for this connector (for example, if the connector is disabled or if an address space not containing addresses of selected devices is selected for the connector).

8. If required, in the **Configure / run** section of the wizard, configure the operation settings for each connector methods (for example, the **Polling via SSH** method requires specifying a port, and a user name and password to connect).

   Methods that require configuring settings appear as expanded blocks. If setting configuration is not required for all connector methods (the default settings are used or no settings are provided for this method), a green icon is displayed next to the connector name.

9. Click **Start**.

   The application starts the process of active device polling.

10. In the **Finish** section of the wizard, click the **Close** button.

    Information about the active polling is displayed in the list of background operations. When this process is complete, the polling results will be available for viewing.

11. To view the results of active polling:

    a. Click the ⤓ button in the menu of the application web interface.

       The list of background operations appears. The list contains separate background operations for each connector that is used for active polling.

    b. After completing each operation, click **Show results** to get the results of the active polling conducted using the corresponding connector.

- Invoking the wizard when working with the network interactions map and the topology map

When working with the network interactions map and the topology map, you can call the active polling configuration wizard for nodes corresponding to the devices known to the application.

To invoke the active polling configuration wizard and run active polling when working with maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Network map** section.

3. On the **Network interactions map** or **Topology map** tab, select one or more nodes for which you want to run active polling of devices. The nodes must represent known devices. You can select no more than 16 devices when configuring and running active polling.

   To select multiple nodes, perform one of the following actions:

   - Hold down the `SHIFT` key and use your mouse to select a rectangular area containing the relevant nodes.

   - Hold down the `CTRL` key and use your mouse to select the relevant nodes.

4. In the toolbar above the network interaction map or the topology map, open the **Perform** drop-down list and select **Active polling**.

   The active polling configuration wizard window opens.

5. If no application user has previously conducted active polling of devices, the wizard window will show a warning regarding the specifics of active polling. Carefully read the warning and confirm that you accept the risks of potential impacts when using the active polling module.

6. In the **Select parameters** section of the wizard, select the check boxes for the specific device information that you want to update using active polling. You can also enable risk detection (the **Risks** check box) and discovery of topology settings for devices (the **Topology settings** check box).

7. In the **Select polling methods** section of the wizard, select the check boxes for the specific methods that you want to use for getting device information, risk detection, and/or reading topology settings.

   The available methods are grouped based on the connectors that provide the capabilities for active polling of devices. The list contains only the methods that are capable of obtaining the selected information. If a connector cannot be used for active polling of selected devices, available methods are not displayed for this connector (for example, if the connector is disabled or if an address space not containing addresses of selected devices is selected for the connector).

8. If required, in the **Configure / run** section of the wizard, configure the operation settings for each connector methods (for example, the **Polling via SSH** method requires specifying a port, and a user name and password to connect).

   Methods that require configuring settings appear as expanded blocks. If setting configuration is not required for all connector methods (the default settings are used or no settings are provided for this method), a green icon is displayed next to the connector name.

9. Click **Start**.

   The application starts the process of active device polling.

10. In the **Finish** section of the wizard, click the **Close** button.

    Information about the running active polling operation is displayed in the list of background operations. When this process is complete, the polling results will be available for viewing.

11. To view the results of active polling:

a. Click the button in the menu of the application web interface.

   The list of background operations appears. The list contains separate background operations for each connector that is used for active polling.

b. After completing each operation, click **Show results** to get the results of the active polling conducted using the corresponding connector.

Performing update polling based on the results of active polling

When active polling of devices is complete, the application analyzes the obtained results and the current (previously saved) device information. If the active polling results suggest the possibility of receiving additional information by running a new active poll, the application will prompt you to run an *update poll*. Update polls are conducted separately for each device that returned results during the first active poll.

To configure and run an update poll:

1. Open the window containing the results of the completed active polling of devices.

   If an update poll is possible for a device, information about this capability is displayed in the **Update polling can be launched with other methods** block.

2. Start the active polling configuration wizard by clicking the link containing the name of the method for receiving relevant device information.

   The active polling configuration wizard window opens. The wizard window will display the **Select polling methods** section with the selected check box for the chosen active polling method.

3. If necessary, configure other settings in the wizard sections and start active polling.

Security audit using Kaspersky Industrial CyberSecurity for Networks

You can use Kaspersky Industrial CyberSecurity for Networks for security audit of the monitored devices. Security audit lets you assess device compliance with security standards and perform other checks (for example, search for vulnerabilities or detect installed software on devices).

Security audit in Kaspersky Industrial CyberSecurity for Networks is performed by running the jobs created for the selected devices. You can manually run security audit jobs or configure a schedule to automatically run each job.

When a job is started, the application initiates a scan of devices covered by this job. You can receive the job execution results by email or view and download the relevant data in the application web interface. Based on the job execution results and on the scans, the application can perform the following actions:

- Generate reports with information about the results.

  The application generates report files in PDF format. If sending reports by email is enabled in the job settings, the application automatically generates reports on each job execution and sends these reports to the specified recipients. If necessary, you can manually generate a report for a completed job or an individual device scan and then export the report to a file.

- Register detected risks of the Vulnerability category.

For the risks registered based on the results of security audit jobs, the application indicates the source of the **OVAL** vulnerability. Such risks are registered by the application if registration of detected vulnerabilities is enabled in the job settings. At the same time, risks with the specified source of **OVAL** vulnerability are registered and processed irrespective of the risks for which other vulnerability sources are specified. Thus, the risk table may display risks with the same CVE ID (or an ID of a different vulnerability database), but with different vulnerability sources.

The security audit jobs must specify the rules used for conducting the audits. Rules can be written in the OVAL language or in the XCCDF language using OVAL definitions.

You can perform device scans as part of a security audit job in one of the following device polling methods:

- **Local agent**.

  You can use this method if Kaspersky Endpoint Agent is installed on the devices selected for the job and integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Kaspersky Endpoint Agent on each device.

- **Remote connection**.

  Use this method if the devices selected for the job do not have Kaspersky Endpoint Agent installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. For this method, in the job settings specify one of the nodes with the installed application components from which connection to the devices is established. Also, specify the credentials for remote connections (credentials are stored in the application as secrets).

Only users with the Administrator role can run security audit jobs.

You can configure security audit and run jobs on the Server web interface page in the **Security audit** section. If the **Remote connection** method is used to scan devices, you can create secrets with the necessary credentials in the **Settings** → **Secrets** section.

When using the security audit function, take into account the following special considerations and limitations:

- This functionality is available after a license key is added.
- Nodes that are used for device scan and have the application components installed must have network access to devices to send and receive data. To provide network access to devices, the node computer must have a network interface providing a connection of these devices to the network. Network interfaces of monitoring points cannot be used for this purpose if these network interfaces receive mirrored industrial network traffic (for example, from SPAN ports of network switches).
- For the **Remote connection** device polling method, the option to strengthen the security of connections with devices by verifying the certificates of these devices is not available. Attackers can attempt to spoof these devices in the network by exploiting the lack of device certificate authentication.

Managing sets of security audit rules

You can manage sets of security audit rules on the **Rule sets** tab in the **Security audit** section.

Only users with the Administrator role can manage the sets of security audit rules.

After creating the list of required sets, you can manage security audit jobs.

Security audit rules

Kaspersky Industrial CyberSecurity for Networks supports security audit rules written in the following languages:

- OVAL (Open Vulnerability and Assessment Language) is an open language for describing vulnerabilities and assessing configurations of information systems. The language standardizes the ways of presenting information, the process of analyzing the system, and the format of the result.

  Rules that use only this language are OVAL definitions which formalize the requirements for information systems, providing the capability to automatically process these requirements.

- XCCDF (Extensible Configuration Checklist Description Format) is an XML-based language for describing checklists of security settings. XCCDF documents usually contain sets of information system requirements.

  Rules that use this language are the lists of high-level requirements in the form of documents with profiles and data groups. For automated processing, such rules must contain associated OVAL definitions.

Security audit rules are grouped into sets. You can use the following types of rule sets:

- System rule sets. These rule sets are supplied and updated together with the database and application module updates. Therefore, before configuring security audit using the system rule sets, install the updates.

- User-defined rule sets. These rule sets are loaded into the application by the user through the import of files.

When a rule set is loaded, the application verifies the rules in the rule set. If errors are detected in the verified rules, the application blocks these rules from being applied. If errors are detected in all rules of the set or the set does not contain any rules, the application blocks the entire set from being applied.

When creating or editing security audit jobs, you can select the rules according to which scans are performed.

Viewing the table with security audit rule sets

The security audit rule set table is displayed on the **Rule sets** tab in the **Security Audit** section.

The rule set settings are displayed in the following columns of the table:

- **ID**

  Rule set ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**.

  The name by which the rule set is represented in the application.

- **Description**

  Description of the rule set.

- **XCCDF publisher**

  Name of the XCCDF document publisher (if specified).

- **XCCDF document version**

  Information about the XCCDF document version (if specified).

- **XCCDF status**

The final status specified for the XCCDF document.

- **XCCDF profiles**

  The number of profiles in the XCCDF document.

- **XCCDF rules in set**

  The number of rules in the XCCDF document.

- **OVAL definitions**

  The number of OVAL definitions.

- **Created**

  Date and time when the rule set was added to the application.

- **Changed**

  Date and time when the rule set was last modified in the application.

- **Origin**

  The type of rule set that determines how the rule set is loaded into the application: system or user rule set.

When viewing the rule set table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Importing sets of security audit rules

You can import security audit rules from files to Kaspersky Industrial CyberSecurity for Networks. Files can contain rules written in the OVAL ? language or in the XCCDF ? language using OVAL definitions.

Imported rule sets are called *custom* rule sets. The **Origin** setting of these rule sets contains the **User** value.

To import files, they must be packed into a ZIP archive. Supported options for the contents of the ZIP archive:

- XCCDF package files that represent an XCCDF document and OVAL definitions in XML format. If the package includes reference files in the CPE (Common Platform Enumeration) format, these files must also be added to the archive.

  The files must be located at the root of the archive. The names of the files in the archive must match the following name masks:

  - `*-xccdf.xml` – mask for the name of the XCCDF document file (for example, SCAP1-xccdf.xml)
  - `*-oval.xml` – mask for the name of the file with OVAL definitions (for example, SCAP1-oval.xml)
  - `*-cpe-dictionary.xml` – mask for the name of the CPE dictionary file (for example, SCAP1-cpe-dictionary.xml)
  - `*-cpe-oval.xml` – mask for the name of the file with OVAL definitions and CPE dictionary (for example, SCAP1-cpe-oval.xml).

- A file that contains OVAL definitions and is not a part of an XCCDF package (the XCCDF document is not required to use the file).

  The file must be located at the root of the archive. The name of the file in the archive must match the mask: `*-oval.xml` (for example, SCAP2-oval.xml).

To import a set of security audit rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Security audit** section.

3. On the **Rule sets** tab, click **Import** on the toolbar.

4. Specify the local path to the ZIP archive using the **Browse** button.

5. Click the **Import** button.

   The data import process starts. Information about the running import operation is displayed in the list of background operations.

6. To switch to a new rule set, perform the following actions:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the import operation to complete.

   c. Click the **Show** button.

Modifying sets of security audit rules

You can modify the names and text descriptions of the custom security audit rule sets. Such changes are not available for system rule sets.

To change the name or the text description of a rule set:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Security audit** section.

3. On the **Rule sets** tab, select the required rule set.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

5. Enter a name and a description for the rule set.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . ‘ - " _`. The rule set name must begin and end with any permitted character except space.

   The rule set name must contain no more than 1,024 characters. The rule set description must contain no more than 4,096 characters.

6. Click **Save**.

Deleting sets of security audit rules

You can delete custom and system security audit rule sets. However, you cannot delete rule sets that have associated security audit jobs.

To delete rule sets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Security audit** section.
3. On the **Rule sets** tab, select the rule sets that you want to delete.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm the deletion of the rule sets.

   You can delete only the rule sets that have no associated security audit jobs. If there are rule sets with associated security audit jobs among the selected rule sets, a corresponding message appears. To delete such rule sets, first delete the associated jobs.

Managing security audit jobs

You can manage security audit jobs on the **Jobs** tab in the **Security audit** section.

After the jobs are started and the device scans are completed, you can get information about the performed scans.

Adding and editing a security audit job

For the existing sets of security audit rules, you can add and edit jobs that the application uses to perform device scans.

Only users with the Administrator role can add and edit security audit jobs.

The security audit job is configured using the Wizard. The Wizard guides you step by step through the configuration of all required job settings. After the configuration is complete, you can wait for the scheduled scans to start on devices or start the scan job manually.

You can invoke the Security Audit Job Configuration Wizard in the following ways:

- **When adding a job for the selected rule set** ?

1. Select the **Security audit** section.
2. On the **Rule sets** tab, select the rule set for which you want to add a security audit job.
3. Click the **Add job** button.

In the Configuration Wizard settings, the selected rule set is specified as default.

- When adding a job with unspecified settings ?

  1. Select the **Security audit** section.
  2. On the **Jobs** tab, click the **Add job** button.

  The Configuration Wizard settings do not have the default values.

- When adding a job based on an existing job ?

  1. Select the **Security audit** section.
  2. On the **Jobs** tab, select the job based on which you want to add a new security audit job.
  3. Click the **Copy** button.

  The default values of the Configuration Wizard settings are set to the values of the existing job settings.

- When adding a job for selected devices ?

  1. Select the **Assets** section.
  2. On the **Devices** tab, select the devices for which you want to add a security audit job.
  3. Right-click to open the context menu.
  4. In the context menu, select **Create security audit job**.

  In the Configuration Wizard settings, a list of devices consisting of the selected devices is generated by default.

- When modifying the selected job ?

  1. Select the **Security audit** section.
  2. On the **Jobs** tab, select the job for which you want to change the settings.
  3. Click the **Edit** button.

The default values of the Configuration Wizard settings are set to the values of the selected job settings.

To configure job settings in the Configuration Wizard window:

1. In the **Select rules** section, do the following:

   a. Select the desired rule set for the job (not available when editing a job).

   b. Specify the profile of the selected rule set.

   c. Select the rules used to perform the scans and, if necessary, specify the desired values for the variables.

2. In the **Select devices** section, create a list of devices to run the scans during the job execution. Select up to 1,000 devices for the job.

   You can create a list of devices using the **Add to job** and **Delete from job** buttons. When you add devices, the application opens a window with a table of devices for selection. You can filter and sort the table to display the desired devices.

3. In the **Job configuration** section, configure the other job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

   The job name must contain no more than 1,024 characters. The job description must contain no more than 4,096 characters.

   b. Select one of the following methods to poll devices:

   - **Local agent**.

     You can use this method if Kaspersky Endpoint Agent is installed on the devices selected for the job and integration between Kaspersky Endpoint Agent and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Kaspersky Endpoint Agent on each device.

   - **Remote connection**.

     Use this method if the devices selected for the job do not have Kaspersky Endpoint Agent installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. For this method, in the job settings specify one of the nodes with the installed application components from which connection to the devices is established. Specify the secret with the credentials for remote connections. You can select only one secret with one set of credentials for the job. In this case, the credentials stored in the selected secret must be applicable on all devices selected for the job (connections to these devices are possible with the same credentials from the secret).

   > For the **Remote connection** device polling method, the option to strengthen the security of connections with devices by verifying the certificates of these devices is not available. Attackers can attempt to spoof these devices in the network by exploiting the lack of device certificate authentication.

   c. If necessary, enable detection of risks of the Vulnerability category based on the job execution results. For this purpose, select the **Register detected vulnerabilities** check box.

   d. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

   - In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, **Monthly**.

- Depending on the selected option, specify the values for the settings to define the precise job start time.

> The application starts the job according to the schedule, provided that the previous start of this job has been completed. If by the time a scheduled job is started its previous launch has the *Running* status, the application skips the start of the scheduled job.

e. To send reports on the job starts by email, enable the **Send by email** option and specify the addresses of the recipients.

The maximum number of report recipients is 10.

4. Click the button to close the Wizard: **Create job** or **Edit job**.

The specified settings are displayed in the job details, on the **Settings**, **Rules**, and **Devices** tabs.

Viewing a table of security audit jobs

The security audit jobs table is displayed on the **Jobs** tab in the **Security audit** section.

The job settings are displayed in the following columns of the table:

- **Job ID**

  Job ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**.

  Name used to represent the job in the application.

- **Description**

  Job description.

- **Created**

  Date and time when the job was added to the application.

- **Changed**

  Date and time when the job was last modified in the application.

- **Rule set**

  The name of the rule set associated with the job.

- **Profile**

  The name of the profile that defines the set of rules and variables for scans during the job execution.

- **XCCDF rules in set**

  The number of selected rules for the job and the total number of rules in the rule set.

- **Devices selected**

  The number of devices selected for the job.

- **Polling method**

  The polling method selected to scan devices: **Local agent** or **Remote connection**.

- **Register vulnerabilities**

  Flag indicating if detection of risks of the Vulnerability category is enabled based on the results of the job.

- **Schedule**

  Information about the schedule according to which the application automatically starts the job.

- **Status of last run**

  The resulting status of all device scans when the job was last run.

- **Last run**

  Date and time when the job was last started.

- **Next run**

  Date and time of the next scheduled start of the job.

When viewing the table of security audit jobs, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Manually starting and stopping security audit jobs

You can manually start and stop security audit jobs. When you start or stop a job, the application starts or stops all scans on the devices selected for this job.

You can stop or start the job depending on the status of the job. For example, a job cannot be started if the status of its last start is *Running*.

Only users with the Administrator role can manually start and stop security audit jobs.

To start a security audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Security audit** section.

3. On the **Jobs** tab, select the job you want to start.

   The details area appears in the right part of the web interface window.

4. Click the **Start** button. The button is disabled if the job cannot be started.

Kaspersky Industrial CyberSecurity for Networks starts the job. You can view information about the device scans in progress on the **Runs** tab in the job details.

To stop a security audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Security audit** section.

3. On the **Jobs** tab, select the job you want to stop.

   The details area appears in the right part of the web interface window.

4. Click the **Stop** button. The button is disabled if the job cannot be stopped.

Stopping a device scan in a security audit job

You can manually stop a device scan as part of the security audit job. When a device scan is stopped, the application does not stop other device scans within this job.

Only users with the Administrator role can manually stop the device scans.

To stop a device scan within a security audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Security audit** section.
3. On the **Jobs** tab, select the job within which you want to stop a device scan.

   The details area appears in the right part of the web interface window.
4. In the details area, go to the **Runs** tab.
5. Select the desired scan and click the **Stop** button in the scan details area that appears. The button is disabled if the scan cannot be stopped.

Deleting security audit jobs

You can delete security audit jobs. However, you cannot delete the jobs with the last run status *Running* or *Pending*.

Only users with the Administrator role can delete security audit jobs.

To delete security audit jobs:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the **Security audit** section.
3. On the **Jobs** tab, select the jobs you want to delete.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm the deletion of the job.

   You can delete only the jobs whose last run status is not *Running* or *Pending*. If there are jobs with the *Running* or *Pending* status among the selected jobs, the corresponding message is displayed. To delete such jobs, first stop the jobs.

Viewing details on the runs of security audit jobs

Kaspersky Industrial CyberSecurity for Networks saves information about the runs of security audit jobs in a database on the Server. Information about the job runs is stored until the jobs are deleted or until the specified limit is exceeded. If the amount of information about the job runs exceeds the specified limit, the application automatically deletes 10% of the oldest records. If the minimum storage time limit is enabled and the application deletes entries whose storage time is less than the defined limit, a corresponding message will appear in the application message log. You can configure the settings for storing information about the job runs.

When working with security audit jobs, you can view general information about job runs and generate reports with the scan results.

Viewing general information about job execution

You can view general information on the job runs in the security audit jobs table. The table displays information about the most recent job runs not including the information about device scans. To view general information on all job runs, including information about the device scans, select the job and in the details area, open the **Runs** tab.

General information about security audit job runs includes the following:

- The job status or the device scan status.

  The following statuses are available:

  - *Pending*—a command to start the scan has not been sent yet.
  - *In progress* – the job is being started or the scan is in progress.
  - *Canceling* – the start of the job or scanning is being stopped.
  - *Canceled* – the start of the job or scanning is stopped.
  - *Completed* – the scan completed successfully or all scans within the job run completed successfully.
  - *Error* – an error occurred during a scan or errors occurred in all scans within the job run.
  - *Partially successful*—the job completed with a partially successful result: some scans have the *Completed* status while some scans have the *Canceled* or the *Error* status.
- Start date and time.
- End date and time.
- Execution duration.

Generating a report on a manual job run

You can manually generate a report on the run of the security audit job. The report stores information about all successful device scans during the selected job run.

The report is generated based on the results of the scans performed on the devices using the security audit rules that are selected in the job settings.

The following reports on the security audit job runs are provided:

- **Full report**.

  This report contains detailed information about the performed scans and the used security audit rules.

- **Executive summary**.

  This report contains a summary of the most important scan results.

To generate a report, the security audit job must have one of the following statuses: *Completed*, *Partially successful*, *Canceled*, or *Error*.

To start generating a report:

1. Select the **Security audit** section.
2. On the **Jobs** tab, select the job for which you want to generate the report.

   The details area appears in the right part of the web interface window.
3. In the details area, go to the **Runs** tab.
4. Select the desired job run.
5. In the job run details area that appears, open the **Get report** drop-down list and select the desired report: **Full report** or **Executive summary**. If the report cannot be generated, the drop-down list is not available.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process.

Go to the **Generated reports** tab in the **Reports** section. The security audit report appears in the table of generated reports. After successful report generation, you can export the generated report to a file.

Generating a report on a manual device scan

You can manually generate a device scan report within a security audit job. The report is generated based on the results of the scans performed on the device using the security audit rules that are selected in the job settings. The report contains detailed information about the performed scans and the used security audit rules.

To generate a report, the device scan must have one of the following statuses: *Completed*, *Canceled*, or *Error*.

To start generating a report:

1. Select the **Security audit** section.
2. On the **Jobs** tab, select the job within which the desired device scan is performed.

   The details area appears in the right part of the web interface window.
3. In the details area, go to the **Runs** tab.
4. Select the desired scan and click the **Get report** button in the scan details area that appears. The button is disabled if the report cannot be generated.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process.

Go to the **Generated reports** tab in the **Reports** section. The security audit report appears in the table of generated reports. After successful report generation, you can export the generated report to a file.

Managing storage settings for the runs of security audit jobs

You can change the specified maximum volume limit for storing information about security audit job runs.

To change the storage settings for the runs of security audit jobs:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the Server tile.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the Server parameters.
5. On the **General** tab, go to the **Security audit** group of settings, and use the **Max volume** setting to define the size limit for storing information about job runs.

   You can select the unit of measure for the space limit: **MB** or **GB**.

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.
6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for information about job runs, and specify the minimum number of days.
7. Click **Save**.

Managing account credentials secrets for remote connections

Secret storage is implemented in Kaspersky Industrial CyberSecurity for Networks. *Secrets* allow you to securely store and use identification and authentication information that the application needs for automatic remote connections to devices. Secrets contain user names with passwords or certificate private keys. With the help of secrets, you can safely use this information in the application without the risk of compromising it.

Secrets are used in security audit jobs for which the **Remote connection** device polling method is selected.

The current version of Kaspersky Industrial CyberSecurity for Networks uses the SSH protocol for remote connections. Keep in the secrets the credentials that are required for remote connections to devices via SSH.

> When using secrets, the option to strengthen the security of connections with devices by verifying the certificates of these devices is not available. Attackers can attempt to spoof these devices in the network by exploiting the lack of device certificate authentication.

Critical information of the secret, such as password or certificate private key, is available to you as plain text only once, when you enter this information when creating the secret. Once a secret is saved, critical information cannot be viewed. You can only replace critical information in the secret when you change the secret, for example, enter a new password.

You can manage secrets in the **Settings** → **Secrets** section.

Only users with the Administrator role can manage secrets.

Adding a secret

You can add up to 500 secrets to the application.

To add a secret:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Secrets**.
3. Open the details area by clicking the **Add secret** link.
4. Enter the secret name.

   The secret name must be unique (must not match the names of other secrets) and must contain from 8 to 256 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The secret name must begin and end with any permitted character except space.
5. Enter the user name to be used for remote connections to devices.

   A user name can contain Latin characters, numbers, periods, and the following special characters: `_` and `-`. The name must begin with a letter, and end with any supported character except a period.
6. Select the secret type:

   - If the secret contains a user password, select the **User password** type and enter the password.

     The password must contain from 8 to 256 ASCII characters.
   - If the secret contains a certificate private key, select the **Private key** type and place the key contents in the text field.

     You can manually enter the sequence of characters comprising the key or upload the key from the certificate file by clicking the **Copy from file** link. Files in the CRT, PEM, CER formats are supported for uploading private keys. If the private key file is protected by a password phrase, before uploading the key enter the password phrase in the **Passphrase** field.

     > To use the certificate private key, copy the certificate public key to all devices to which the remote connections using the secret are established. Copying the public key to devices is performed without the participation of Kaspersky Industrial CyberSecurity for Networks.
7. If necessary, enter an additional password in the **Root user password** field.

An additional password may be required for scans based on certain security audit rules which are used when connecting to the network equipment with administrator privileges (with root privileges). In such cases, access is requested on behalf of the root account or on behalf of the account that is set on the network equipment to process requests with administrator privileges.

8. Click **Save**.

Viewing the secret table

The table of remote connection secrets is displayed in the **Settings** → **Secrets** section of the application web interface.

Information about secrets is displayed in the following columns of the table:

- **Name of secret**.

  Name used to represent the secret in the application.

- **Created**.

  Date and time when the secret was added to the application.

- **Changed**.

  Date and time when the secret was last modified in the application.

When viewing the secrets table, you can use the configuration, filter, search, and sort functions.

Changing the settings of a secret

When changing the settings of the secret, you can change the name of the secret, the user name, and replace the certificate password and/or private key in the secret with new values.

After the secret settings, including the secret name, are changed, the new settings are applied in the security audit jobs where the secret is used.

To edit the secret settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Secrets**.

3. Select the secret you want to change.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

5. Change the settings as necessary. The options available when changing the secret settings are the same as the ones when adding a secret.

   Critical secret information, such as passwords and certificate private keys, is not displayed as plain text. You can only replace the critical information with new information by using the links above the credentials fields.

Deleting secrets

You can delete secrets from the Kaspersky Industrial CyberSecurity for Networks secrets repository.

Before deleting a secret, it is recommended to specify a different secret or polling method in the security audit jobs that use this secret. If a deleted secret is specified in the security audit job, errors occur the next time the job is run.

To delete secrets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Secrets**.
3. Select the secrets you want to delete.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm the deletion of the secrets.

Forming a topology map

A topology map is a visual representation of the physical connections between devices in the industrial network. In contrast to the network interactions map, the topology map is intended for displaying the actual connections between devices via network cables connected to the ports of network interfaces. After generating a topology map, you will see one or more graphs that visually display the structure of connections between devices via network equipment such as switches, hubs, routers, and others.

The following objects may be displayed on the topology map:

- Nodes. These objects represent devices and network equipment.
- Links. These objects represent the physical connections between nodes.

Nodes are constantly displayed on the topology map regardless of whether or not these nodes have connections to other nodes. Nodes can be filtered for a more convenient display. Nodes are also distinguished in various ways on the topology map depending on their types, statuses, and events related to the nodes.

After links are added for nodes, you can arrange these nodes on the topology map according to a topology generation procedure.

The topology map is displayed on the **Topology map** tab in the **Network map** section.

Data for adding connections to the topology map can be obtained automatically based on the results of active polling of devices – if the corresponding polling methods are used (for example, polling via SNMP). You can also add connections manually.

Nodes on the topology map

Nodes on the topology map can be of the following types:

- A device that is known to the application. This type of node represents a device that is listed in the devices table.
- Unmanaged switch. This type of node represents a device whose MAC- and IP addresses are either unavailable or unknown. Due to its lack of address information, this device cannot be added to the devices table. However, such a device can still be linked to other devices. For instance, this type of node may appear on the topology map if active polling detects multiple connections of different devices to one port of the same device. If this is the case, the application determines that an unidentified switching device (such as a hub) is present in the network, and automatically creates a node for this device. No more than 1,000 unmanaged switches can be added to the application.

  If you are able to identify the MAC- and/or IP address of a node for an unmanaged switch, you can use this unmanaged switch node to manually add a new device to the devices table.

Displayed information on nodes representing devices

The following information is displayed for nodes representing known devices when the topology map scale is maximized:

- Assigned device name.
- Device category icon.
- Network name or address of the device (if an IP address is not assigned, the MAC address is displayed).
- Various icons depending on fulfillment of the following conditions:
  - If the router indicator has been set for the device.
  - If an EPP application is installed on the device (the color of the icon depends on the connection state).
  - If the device has the *Archived* status.
- The thick line on the left border of a node has one of the following colors depending on the device's security state:
  - Green signifies the *OK* security state.
  - Yellow signifies the *Warning* security state.
  - Red signifies the *Critical* security state.

If a device has the *Unauthorized* status, the node has a red background.

Displayed information on nodes representing unmanaged switches

The following information is displayed for the nodes representing unmanaged switches when the topology map scale is maximized:

- Defined node name.
- Unmanaged switch icon.

Nodes representing unmanaged switches have a gray background.

Links on the topology map

Links on the topology map show the physical connections between nodes. Each link represents a connection between ports of network interfaces on devices connected via network cable.

Links are displayed as horizontal or vertical lines on the topology map. Multiple link lines extending from one node on shared sections of the map are displayed as a thick line representing a network bus.

Viewing details about objects on the topology map

Detailed information about objects presented on the topology map is displayed in the details area. To display details, you can select an object by clicking it.

The following information is displayed for the selected node:

- If a node represents a known device, the details area displays the same information that is displayed when selecting a device in the devices table.
- If a node represents an unmanaged switch, the details area displays the following information:
  - Name of the unmanaged switch node
  - Type of node (Unmanaged switch)
  - **Topology settings** section containing a list of ports for which links with other nodes were added or may be added

Name of one of the link nodes and list of ports of this node with connections to other nodes is displayed for the selected connection. If a bus is selected, you will see a list of ports of the node that has the highest number of links in the selected bus.

Adding nodes to the topology map

When generating a topology map, the application can automatically add detected nodes to the topology map. If some relevant nodes were not automatically added by the application, you can manually add them when working with the topology map.

Only users with the Administrator role can manually add nodes.

If you know the MAC- and/or IP address of a device that you want to add to the topology map as a node, you can manually add this device. If the address information of a node is unknown or missing (for example, if the device is a hub), you can add an unmanaged switch node.

To add an unmanaged switch to the topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. On the **Topology map** tab in the **Network map** section, select **New unmanaged switch** in the **Add node** drop-down list.

   A details area with the unmanaged switch settings appears in the right part of the window.

3. Enter the node name.

   The node name must be unique (must not match the names of other unmanaged switches) and must contain no more than 100 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. The node name must begin and end with any permitted character except a space.

4. Click **Save**.

The unmanaged switch node will appear on the topology map. Then you will be able to add links with this node for other nodes.

Manually adding links to the topology map

You can manually add links and configure their settings when working with the devices table or topology map.

Only users with the Administrator role can add links and configure their settings.

You can use the following functions when adding links to the topology map:

- **Adding links for a selected node and configuring additional topology settings** ?

This function is convenient if you want to add multiple links with other nodes for one node (for example, add all links for a switch). When using this method for adding links, you can also configure all topology settings for the device.

To add links for a node and configure additional topology settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the node on the **Topology map** tab in the **Network map** section.

   You can also select the device represented by the relevant node on the **Network interactions map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select an unmanaged switch node.

   The details area appears in the right part of the web interface window.
3. In the upper right corner of the details area, click the ⋮ icon and select **Topology settings** → **Configure settings**.

   The window for configuring the ports and connections of the selected node is displayed.
4. In the **Physical ports** settings group, add information about links with other nodes. Information about each link must be provided in a separate line in which you can specify the following settings:
   - Name of the physical port where the network cable is connected (optional setting)
   - VLAN IDs (optional setting)
   - Addresses of the network interface connected to the port (optional setting)
   - Node that will serve as the second side of the connection (to select a node, you will see a window containing the table of available nodes and ports on nodes)
5. If necessary, provide information on the virtual ports of the device in the **Virtual ports** settings group.

   Information on virtual ports is not used for generating the topology map.
6. Click **Save**.

- Adding links for selected nodes without configuring additional topology settings

This function is convenient if you want to add links of multiple nodes with one node (for example, add a link with one switch for each of the selected nodes). When using this method for adding links, the additional settings of these links will remain undefined. For instance, you cannot select a port on the node for connections to be added. You can configure the additional settings of links after they are added when editing the topology settings for a node.

Links can be added if no more than 50 rules are selected.

To add links for nodes without configuring additional settings of links:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select one or more nodes on the **Topology map** tab in the **Network map** section.

   To select multiple nodes, perform one of the following actions:

   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.

   You can also select devices represented by the relevant nodes on the **Network interactions map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select nodes of unmanaged switches.
3. Right-click to open the context menu.
4. In the context menu, select **Add connection with node**.

   You will see a window containing a table of nodes available for selection.
5. Select the relevant node in the table and click **OK**.

Editing the topology settings for a node

When editing topology settings, you can add, configure, and delete links for a node, and configure settings of the virtual nodes.

Only users with the Administrator role can edit topology settings.

To configure the topology settings for a node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select the node on the **Topology map** tab in the **Network map** section.

   You can also select the device represented by the relevant node on the **Network interactions map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select an unmanaged switch node.

   The details area appears in the right part of the web interface window.

3. In the upper right corner of the details area, click the ⋮ icon and select **Topology settings** → **Configure settings**.

   The window for configuring the ports and connections of the selected node is displayed.

4. In the **Physical ports** settings group, provide information about links with other nodes. Information about each link must be provided in a separate line in which you can specify the following settings:

   - Name of the physical port where the network cable is connected (optional setting)
   - VLAN IDs (optional setting)
   - Addresses of the network interface connected to the port (optional setting)
   - Node that will serve as the second side of the connection (to select a node, you will see a window containing the table of available nodes and ports on nodes)

5. If necessary, provide information on the virtual ports of the device in the **Virtual ports** settings group.

   Information on virtual ports is not used for generating the topology map.

6. Click **Save**.

Renaming the node of an unmanaged switch

You can rename an unmanaged switch node added to the topology map either automatically or manually.

Only users with the Administrator role can rename a node of an unmanaged switch.

To rename an unmanaged switch node on the topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. On the **Topology map** tab in the **Network map** section, select the unmanaged switch node.

   The details area appears in the right part of the web interface window.

3. Click the **Edit** button.

4. In the field containing the current name of the node, enter a new name.

   The node name must be unique (must not match the names of other unmanaged switches) and must contain no more than 100 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. The node name must begin and end with any permitted character except a space.

5. Click **Save**.

Deleting objects from the topology map

You can delete nodes and connections when working with a topology map. When nodes representing known devices are deleted, the devices are deleted from the devices table.

Only users with the Administrator role can delete objects from the topology map.

To delete a node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, select the node you want to delete.

   The details area appears in the right part of the web interface window.
3. Click the **Delete** button.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm removal of the selected node.

To delete a link or bus (multiple links):

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, select the link or bus.
3. Click the **Delete** button.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm removal of the selected links.

Changing the topology map scale

The topology map can be displayed in a scale of 1–100%. The current scale value is displayed in the toolbar located in the left part of the topology map display area.

To change the scale of the topology map:

Use the mouse wheel or the **+** and **–** buttons located in the toolbar next to the current scale value.

Reducing the scale of the map reduces the amount of information that is displayed in nodes.

If the display scale is less than 25%, icons and text information are not displayed in nodes. With this reduced scale, on each node representing a known device, the upper-right corner displays the device status as a triangle in one of the following colors:

- Green signifies that the device has the *Authorized* status.
- Red signifies that the device has the *Unauthorized* status.
- Gray signifies that the device has the *Archived* status.

Positioning of the topology map

If necessary, you can change the positioning of the topology map either manually or automatically. Automatic positioning lets you move the map and change its scale in such a way to display all nodes that satisfy the defined filter settings.

To manually position the topology map:

1. Position the mouse cursor over any part of the topology map that is not occupied by objects.
2. Click and hold the left mouse button to drag the topology map image.

To automatically position the topology map:

Click the button in the toolbar located in the left part of the topology map display area.

The positioning and scale of the map will change to display all nodes.

Pinning and unpinning nodes on the topology map

By default, nodes are not pinned on the network map. Unpinned nodes may be automatically arranged for optimal display of other objects.

Nodes are pinned when their location is changed manually. You can also pin the current location of displayed objects without moving them.

To pin and unpin objects without moving them, you can use the buttons in the toolbar located in the left part of the topology map display area. You can use the and buttons to pin and unpin all nodes displayed on the topology map. The buttons are available if the topology map contains objects for which the corresponding actions can be applied.

After the location of a node is pinned, the icon appears in the upper-right corner of this element (if the topology map has a scale of less than 25%). You can also use this icon to unpin the object.

The location of a pinned node is retained. If a pinned node disappears from the topology map (for example, after a filter is applied), this node will be displayed in the same location the next time it appears (or nearby, if this place is already occupied by another pinned node).

Manually changing the location of nodes on the topology map

You can manually change the location of nodes on the topology map by using the arrangement method that is most convenient for you.

After their arrangement, nodes are pinned in their new location. If necessary, you can unpin these objects.

To change the position of nodes on the topology map:

1. On the topology map, select one or multiple nodes.

   To select multiple nodes, perform one of the following actions:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

2. Use your mouse to drag the selected objects to the necessary location.

   After they are moved, nodes remain pinned. The 📌 icon appears in these objects.

Automatically arranging nodes on the topology map

For optimal arrangement of objects on the topology map, you can use an algorithm to automatically change the location of nodes (auto-arrange). This algorithm lets you arrange unpinned nodes that have links with other nodes according to the topological hierarchy.

To arrange nodes on the topology map:

Click the ≐ button in the toolbar located in the left part of the topology map display area.

After automatic arrangement, unpinned nodes will not be pinned in their new locations. If necessary, you can manually pin these objects.

Filtering objects on the topology map

To limit the number of nodes displayed on the topology map, you can use the following functions:

- **Filtering by device status**

  1. In the toolbar located above the topology map, open the **Device statuses** drop-down list.

     You will see a list containing the names of statuses for known devices (**Unauthorized**, **Authorized**, **Archived**), and the **Unmanaged switch** status for unmanaged switches.

  2. In the drop-down list, select the check boxes for the statuses of devices that need to be displayed on the topology map.

  3. Click **OK**.

  The topology map will display only those nodes that have the selected statuses.

- **Filtering by device security state**

  1. In the toolbar located above the topology map, open the **Device states** drop-down list.

     You will see a list containing the names of security states for devices (**OK**, **Warning**, **Critical**).

  2. In the drop-down list, select the check boxes for the security states of devices that need to be displayed on the topology map.

  3. Click **OK**.

  The topology map will display only those nodes that represent devices with the selected security states.

- **Filtering by device category**

1. In the toolbar located above the topology map, open the **Device categories** drop-down list.

   You will see a list containing the names of categories for known devices, as well as an individual category for unmanaged switches.

2. In the drop-down list, select the check boxes for the categories of devices that need to be displayed on the topology map.

3. Click **OK**.

The topology map will display only those nodes that represent the selected categories of devices.

- Filtering by VLAN ID in topology settings ?

1. In the toolbar located above the topology map, open the **VLAN ID** drop-down list.

   You will see a window containing a field for entering VLAN IDs.

2. Enter one or more VLAN IDs of devices that need to be displayed on the topology map.

   You can specify several identifiers separated by comma or as a range (for example: `1, 2, 4-6, 8`).

3. Click **OK**.

The topology map will display only those nodes whose topology settings include ports with the defined VLAN IDs.

- Enabling and disabling the display of nodes that do not have links to other nodes ?

By default, the topology map displays all nodes regardless of whether they have links to other nodes. If necessary, you can disable the display of all nodes that do not have links with other nodes on the topology map.

To enable or disable the display of nodes that do not have links to other nodes:

Use the **Display unlinked nodes** toggle button in the toolbar located above the topology map.

- Resetting the filter settings ?

You can reset the defined node filtering settings to their default state.

To reset the defined filter settings on the topology map:

In the toolbar located above the topology map, click the **Default filter** button (this button is displayed if filter settings have been defined).

Saving and loading topology map display settings

The application lets you save the current topology map display settings. A set of saved display settings is called a *view*. You can use views to apply their saved settings on the topology map (for example, to quickly restore the display settings after making some changes, or to work with the topology map on a different computer).

When a topology map view is saved, the following display settings are saved:

- Scale
- Positioning of the topology map
- Location of pinned nodes
- Filtering of nodes

The application can save and use no more than 10 groups of settings providing different topology map views.

Only users with the Administrator role can manage the list of topology map views (including saving the current display settings). However, users with the Administrator role and users with the Operator role can both access the list of views and apply the saved groups of settings.

When working with topology map views, you can use the following functions:

- **Adding a new view while saving the current topology map display settings**

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
  2. On the **Topology map** tab in the **Network map** section, configure the topology map display settings.
  3. Open the **Configure network map views** window by clicking the **Manage views** button.
  4. Click **Add**.
  5. Type the view name in the entry field.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     A view name must meet the following requirements:

     - Must begin and end with any permitted character except a space.
     - Must contain 100 characters or less.
     - Must not match the name of a different view (not case-sensitive).
  6. Click the ✓ icon on the right of the entry field.

- **Updating a view while saving the current topology map display settings**

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, configure the topology map display settings.
3. Open the **Configure network map views** window by clicking the **Manage views** button.
4. Select the view in which you want to save the current topology map display settings.
5. Click the **Overwrite** button.

   A window with a confirmation prompt opens.
6. In the prompt window, confirm that you want to save the current settings in the selected view.

- Renaming a topology map view

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
  2. On the **Topology Map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
  3. Select the view that you want to rename.
  4. Click the ✎ icon on the right of the current view name.
  5. In the entry field, enter the new name of the view.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     A view name must meet the following requirements:

     - Must begin and end with any permitted character except a space.
     - Must contain 100 characters or less.
     - Must not match the name of a different view (not case-sensitive).
  6. Click the ✓ icon on the right of the entry field.

- Deleting a topology map view

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology Map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
3. Select the view that you want to delete.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the selected view.

- Applying saved view settings on the topology map ⓘ

1. On the **Topology Map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
2. Select the relevant view in the list.
3. Click the **Apply** button.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm application of the view.

Search for nodes on the topology map

You can search nodes on the topology map based on information about these nodes. This search will involve all nodes that meet the current filter settings, including those located outside of the displayed part of the topology map.

For nodes representing known devices, the search is performed in all columns of the devices table except the following columns: **Status**, **Security state**, **Last seen**, **Last modified**, and **Created**. The search is also performed in the values of custom fields for devices.

To find relevant nodes on the topology map:

On the **Topology Map** tab in the **Network map** section, enter your search query into the **Search nodes** field. The search is initiated as you type characters in the search field.

If nodes that satisfy the search query are found, the contours of these nodes are highlighted in yellow. However, the right part of the **Search nodes** field will display the following items:

- Sequence number of the currently selected node among the search results.
- Total number of nodes found.
- Arrows for moving between found nodes. Arrow movements proceed in alphabetical order of the names of found objects. When moving to the next node, the topology map is automatically positioned to display this

node.

Configuring event types

Event types define the settings used when registering events, including their titles, descriptions, base scores, and registration settings. In Kaspersky Industrial CyberSecurity for Networks, you can view the settings of event types, change the settings of event types, and configure automatic saving of traffic and transmission of registered events via connectors.

Viewing the table of event types

The event types provided in the application are displayed under **Settings** → **Event types** in the application web interface.

The table of event types contains *system event types*. These event types are created by the application during installation and cannot be deleted from the list. Various sets of system event types are used for the event registration technologies employed in the application.

Some system event types can be used as the basis for configuring *user-defined settings of events* that will be used when registering events in specific cases. User settings can be defined for the following event types:

- Event type based on Deep Packet Inspection technology with the code 4000002900 – for registering events based on Process Control rules.
- Event type based on External technology with the code 4000005400 – for registering events using the Kaspersky Industrial CyberSecurity for Networks API.

User-defined settings take priority when registering events. The settings defined in system event types are used if no user settings are defined.

The following settings are available for event types:

- **Code** – unique number (identifier) of the event type. In the event types table, the number is displayed together with the event title in the **Code and title** column. In the table of registered events, the event type identifier is displayed in the **Event type** column.
- **Title** – contents of the event title presented as text and/or variables. System event types may utilize specific variables only for these event types (for example, the `$systemCommandShort` variable in the event type for Command Control technology) or common variables that can also be used in user-defined settings (for example, the `$top_level_protocol` variable in the event type for Network Integrity Control technology). In the event types table, the content of the title is displayed together with the event type number in the **Code and title** column. In the table of registered events, the text of the title and/or received values of variables are displayed in the **Title** column.
- **Base score** is the initial value for calculating the score of the registered event. If an event type can have different base scores, then the maximum value is displayed. This setting is displayed in the event types table.
- **Technology** – technology used for event registration. This setting is displayed in the event types table.
- **Description** – additional text that describes the event type. Like the title, a description may contain variables. This setting is not displayed in the event types table (you can view the description in the details area of the

selected event type). In the table of registered events, the text of the description and/or received values of variables are displayed in the **Description** column.

- **<Recipient connector name>** – name of the connector that the application uses to forward events to the recipient system. The application sends recipient systems only those types of events that are configured for forwarding through the connector. Each connector configured to forward events to the third-party systems is displayed in a separate column of the risk types table. This setting is not displayed in the details area for the selected event type.
- **Event regeneration period** – maximum period of time after which an event is allowed to be registered again. If the conditions for event registration are repeated before the specified time period elapses, a new event is not registered but the counter for the number of repeats of the previously registered event is increased and the date and time of the last occurrence of the event is updated. After this period elapses, the application will register a new event of this type when the event registration conditions are repeated. The repeat event timeout period begins when an event of this type is last registered. For example, if the defined time period is 8 hours and the conditions for registering this type of event are detected two hours after the previous event, a new event will not be registered. A new event will be registered when the event registration conditions are detected after 8 or more hours. This setting is not displayed in the event types table (you can view and configure this setting in the details area of the selected event type).

  > For registered events, the event regenerate period may occur earlier than the specified period. Re-registration of an event is allowed earlier than the defined period if the *Resolved* status is assigned to the event, and if the computer performing Server functions was restarted.

- **Save traffic** – this setting enables or disables automatic saving of traffic when an event is registered. This setting is not displayed in the event types table (you can view and configure this setting in the details area of the selected event type).

  > If automatic saving of traffic is disabled, you can manually load traffic some time after registration of an event of this type. When the application receives a request to load traffic, it searches network packets in traffic dump files that were temporarily created by the application. If relevant network packets are found in the traffic dump files, they are loaded after first being saved in the database.

When viewing the event types table, you can use the configuration, filter, search, and sorting functions.

Editing the settings of a system event type

To edit the settings of a system event type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Event types**.
3. In the table of event types, select the event type that you want to edit.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.
5. Configure the editable settings, such as the event regeneration period and settings for saving traffic.

6. Click **Save**.

Configuring automatic saving of traffic for system event types

When editing event types, you can enable or disable automatic saving of traffic for events when they are registered. If traffic saving is enabled, the network packet that caused the event registration is saved to the database, as well as the packets received before and after the event registration and detected within the network session in which the event was registered. The settings for saving traffic determine the number of saved network packets and time limits.

If automatic saving of traffic is disabled for an event type (and user-defined settings enabling autosaving of traffic are not defined for this event type), you will be able to manually load traffic only after waiting some time after registration of an event of this type. In this case, the application uses traffic dump files to load traffic (these files are temporarily saved and are automatically deleted as more and more traffic is received). When traffic is loaded from these files, the database saves the specific amount of network packets that was defined by default when enabling the saving of traffic for event types.

> The application saves traffic in the database only when an event is registered. If the conditions for registering this event are repeated during the event regenerate timeout, traffic at this point in time is not saved in the database.

You can enable and configure the saving of traffic for any event types except a system event type assigned the code 4000002700. An event with the code 4000002700 is registered when there is no traffic at a monitoring point. For this reason, traffic is not expected for this type of event.

If saving of traffic is enabled for incidents (meaning for a system type of event that is assigned the code 8000000001), the application saves traffic for all embedded events of an incident when the incident is registered. The settings defined for the incident are applied when saving traffic of embedded events. However, the traffic storage settings defined directly for event types embedded in an incident take priority over the settings defined for an incident. This means that traffic for embedded events of an incident will be saved according to the settings defined for the specific types of these events. If these settings are not defined, the traffic for embedded events will be saved according to the settings defined for an incident.

To enable and configure the settings for saving traffic for an event type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Event types**.

3. In the table of event types, select the event type that you want to edit.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

5. Select the **Save traffic** toggle switch to *Enabled*.

6. Configure saving of traffic before event registration. To do so, specify the necessary values in the **Packets before event** and/or **Time to event, ms** fields. If the value is zero, the setting is not applied. If the values are defined in both of these fields, the application will save the minimum amount of packets corresponding to one of the defined values.

7. Configure the saving of traffic after event registration. To do so, specify the necessary values in the **Packets after event** and/or **Time after event, ms** fields. If the value is zero, the setting is not applied. If the values are defined in both of these fields, the application will save the minimum amount of packets corresponding to one of the defined values.

   > For certain technologies (particularly Deep Packet Inspection), fewer post-registration packets than defined by the settings for saving traffic may be saved in events. This is due to the technological specifics of traffic monitoring.

8. Click **Save**.

Configuring forwarding of events via connectors

When configuring system event types, you can specify the connectors through which Kaspersky Industrial CyberSecurity for Networks will forward registered events to recipient systems (for example, to Kaspersky Security Center). Kaspersky Industrial CyberSecurity for Networks can relay event information through multiple connectors simultaneously.

To configure forwarding of events through connectors to recipient systems:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Event types**.

3. Make sure that the event types table displays columns with the relevant connectors.

   If a column with the required connector is not available, check the column display settings. If the connector has not been added to the list of connectors, add it.

4. In the event types table, select the event types for which you want to enable or disable forwarding via connectors.

   If you select one event type, the details area appears on the right part of the web interface window.

5. Do one of the following:

   - If you select one event type, click the **Select connectors** button in the details area.

   - If you select several event types, click the **Select connectors** button in the upper part of the window.

   The **Event recipient connectors** window opens.

6. Select the check boxes next to those connectors that you want to use to forward events to recipient systems.

7. Click **OK**.

Common variables for substituting values in Kaspersky Industrial CyberSecurity for Networks

You can use common values to substitute current values in Kaspersky Industrial CyberSecurity for Networks. You can use common variables in the following settings:

- Titles and descriptions of events in user-defined settings for registering events (for example, in Process Control rules).
- Settings for forwarding events, application messages or audit entries via the email connector.

To insert a common variable into the entry field:

Start entering the name of the variable beginning with the $ character and choose the appropriate common variable in the list that appears.

Depending on their purpose, common variables can be used to substitute values in various settings (see the table below).

Common variables for value substitution

Variable	Purpose	Where it is used
`$communications`	Strings describing network interactions (one line for each network interaction) indicating the protocol and addresses of the network packet source and destination.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$dst_address`	Address of the network packet destination (depending on the data available in the protocol, this can be an IP address, port number, MAC address and/or other address data).	• User-defined settings for registering events.
`$extra.<paramName>`	Additional variable added using the `AddEventParam` function for an external system or Lua script.	• User-defined settings for registering events.
`$rule_max_value`	Assigned maximum value in the Process Control rule.	• User-defined settings for registering events.
`$rule_min_value`	Assigned minimum value in the Process Control rule.	• User-defined settings for registering events.
`$monitoring_point`	Name of the monitoring point whose traffic invoked registration of the event.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$occurred`	Date and time of registration.	• User-defined settings for registering events. • Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$protocol`	Name of the application-layer protocol that was being monitored when the event	

	was registered.	• User-defined settings for registering events.
`$src_address`	Address of the network packet source (depending on the data available in the protocol, this can be an IP address, port number, MAC address and/or other address data).	• User-defined settings for registering events.
`$tags`	List of all names and values of tags indicated in the Process Control rule.	• User-defined settings for registering events.
`$technology_rule`	Name of the rule in the event.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$top_level_protocol`	Name of the top-level protocol.	• User-defined settings for registering events.
`$type_id`	Code of the event type, application message, or audit entry.	• User settings for registering events (the `$event_type_id` variable may also be used). • Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$rule_values`	List of values of the Process Control rule (authorized or unauthorized).	• User-defined settings for registering events.
`$closed`	Date and time when the *Resolved* status was assigned or the date and time of the event regeneration period (for events that are not incidents), or the date and time of registration of the last event included in the incident (for incidents).	• Settings for forwarding events through a connector.
`$count`	Number of times an event or incident was triggered.	• Settings for forwarding events through a connector.
`$description`	Description	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$id`	Unique ID of the registered event, application message, or audit entry.	• Settings for forwarding events through a connector.

		• Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$message_category`	Category of transmitted data (event, application message, or audit entry).	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$message_count`	Number of transmitted events, application messages or audit entries.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$messages`	Template that consists of a block containing a list of data.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$node`	Node with the installed application component that sent the data.	• Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$result`	Operation result in the audit entry.	• Settings for forwarding audit entries through a connector.
`$score`	Event score value.	• Settings for forwarding events through a connector.
`$severity`	Event severity level.	• Settings for forwarding events through a connector.
`$status`	Application message status.	• Settings for forwarding application messages

		through a connector.
`$system_process`	Application process that invoked message registration.	- Settings for forwarding application messages through a connector.
`$technology`	Technology associated with the event.	- Settings for forwarding events through a connector.
`$title`	Event title, message text, or registered action.	- Settings for forwarding events through a connector. - Settings for forwarding application messages through a connector. - Settings for forwarding audit entries through a connector.
`$user`	Name of the user that performed the registered action.	- Settings for forwarding audit entries through a connector.

Configuring risk types

Risk types define the settings used when registering risks in Kaspersky Industrial CyberSecurity for Networks: names, categories, and base scores for risks. You can view the settings of risk types and edit the values of base scores for certain types of risks if necessary.

> After the application is installed, the original list of risk types is used. You can update and expand the supported risk types by installing updates.

Viewing the table of risk types

The table of risk types is displayed under **Settings** → **Risk types** in the application web interface.

The settings of risk types are displayed in the following columns of the table:

- **Code**.

  Unique number of the risk type. In the table of registered risks, the number of a risk type is displayed in the details area of the selected risk.

- **Name**

The name of the risk type displayed in the risk type table. When a risk is registered, its name may not fully match the name of the risk type used. The names of some risk types can be completely replaced by other names for registered risks. For instance, risk types with such names include risks of the **Risk from external system** types. If this type of risk is used to register a risk, the application saves the risk name specified in the risk information source (for example, in a third-party application that uses Kaspersky Industrial CyberSecurity for Networks API).

- **Category**

  Name of the risk category.

- **Base score**

  Initial value for calculating the score of the registered risk. The defined values for base scores are applied when registering all risks except risks from external systems. Risk types named **Risk from external system** have zero values for their base scores. The base scores for these risks must be specified in the recipient applications that register risks using the Kaspersky Industrial CyberSecurity for Networks API.

When viewing the table of risk types, you can use the configuration, filter, search, and sorting functions.

Changing the base score for a risk type

Base scores cannot be changed for risk types named **Risk from external system**. If such a risk type is used to register a risk, the base score of this risk must be defined from the source of information about the risk (for example, by the recipient application using the Kaspersky Industrial CyberSecurity for Networks API).

To change the base score for a risk type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Risk types**.
3. In the table of risk types, select the risk type whose base score you want to edit.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.
5. Specify the necessary value for the base score.
6. Click **Save**.

Managing the settings for storing risks

You can change the limits on the maximum space used for storing risks.

To edit risk storage settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.

3. Select the Server tile.

   The details area appears in the right part of the web interface window.

4. Click the **Edit** button.

   The details area will show the tabs for configuring the Server parameters.

5. On the **General** tab, go to the **Risks** group of settings and use the **Max volume** setting to define the size limit for storing risks data.

   You can select the unit of measure for the space limit: **MB** or **GB**.

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for risks, and specify the minimum number of days.

7. Click **Save**.

Managing reports and report templates

Kaspersky Industrial CyberSecurity for Networks can generate reports containing information about the states of devices and system security, monitored technological process parameters and system commands, and information about detected risks and interactions with third-party devices. The application generates report files in PDF format based on *report templates*. A report template is a set of parameters determining the conditions for generating a report. Templates can be system templates (created during installation of the application) or user-defined templates (created by duplicating templates).

In the **Reports** section, a user with the Administrator role can duplicate templates to create user-defined report templates, edit and delete report templates, delete generated reports, and cancel report generation.

Kaspersky Industrial CyberSecurity for Networks can also generate reports with the device scan results as a part of a security audit job, as well as reports on the runs of security audit jobs. Reports generation is started in the **Security audit** section. You can view the generated reports on the **Generated reports** tab.

Duplicating a report template

In the current version of Kaspersky Industrial CyberSecurity for Networks, you can create user-defined templates by duplicating existing report templates. You can duplicate system templates and user-defined templates. When duplicating a template, you cannot change the composition and layout of information blocks in a report.

The maximum number of templates in the application is 5,000.

Only users with the Administrator role can duplicate report templates.

To duplicate a report template:

1. Select the **Reports** section.

2. On the **Report templates** tab, select the relevant template.

   The details area appears in the right part of the web interface window.

3. Click the **Create new template** button.

4. In the **Name** field, enter the name of the report template.

   You can use letters of the English and Russian alphabets, numerals, a space, and the characters -, – and _.

   The report template name must meet the following requirements:

   - Must not match the name of another report template (not case-sensitive).

   - Must contain 100 characters or less.

   The names of reports generated based on the updated template will match the new name of the template.

5. In the **Data period** drop-down list, select the time period for which you want to obtain system information in the report.

   You can generate reports containing information received by the application over the past 24 hours, 7 days, 30 days, year, or a manually defined period.

6. If you need to generate reports according to a schedule, turn on the **Generating a report by schedule** toggle button and configure the schedule settings:

   a. In the **Frequency** drop-down list, choose how often to generate a report: **Hourly**, **Daily**, **Weekly**, **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise time to start report generation.

7. If necessary, use the **Recipient addresses** field to enter the email address to which you want to send the generated reports. If you need to specify additional recipients of the report, click the **Add recipient address** button and enter the email address.

   The maximum number of report recipients is 20.

8. Click **Save**.

The new report template will appear in the report templates table.

Editing a report template

Only users with the Administrator role can edit report template settings.

To edit report template settings:

1. Select the **Reports** section.

2. On the **Report templates** tab, select the relevant template.

   The details area appears in the right part of the web interface window.

3. Click the **Edit** button.

4. In the **Name** field, enter the name of the report template.

   You can use letters of the English and Russian alphabets, numerals, a space, and the characters -, – and _.

   The report template name must meet the following requirements:

   - Must not match the name of another report template (not case-sensitive).

- Must contain 100 characters or less.

The names of reports generated based on the updated template will match the new name of the template.

5. In the **Data period** drop-down list, select the time period for which you want to obtain system information in the report.

   You can generate reports containing information received by the application over the past 24 hours, 7 days, 30 days, year, or a manually defined period.

6. If you need to generate reports according to a schedule, turn on the **Generating a report by schedule** toggle button and configure the schedule settings:

   a. In the **Frequency** drop-down list, choose how often to generate a report: **Hourly**, **Daily**, **Weekly**, **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise time to start report generation.

7. If necessary, use the **Recipient addresses** field to enter the email address to which you want to send the generated reports. If you need to specify additional recipients of the report, click the **Add recipient address** button and enter the email address.

   The maximum number of report recipients is 20.

8. Click **Save**.

The changes will be displayed in the corresponding columns of the report templates table.

Deleting a report template

> Only user-defined report templates can be deleted.

Only users with the Administrator role can delete report templates.

To delete a report template:

1. Select the **Reports** section.

2. On the **Report templates** tab, select one or more report templates that you want to delete.

3. Click the **Delete** button.

   You cannot delete system report templates. In the report templates table, system templates are displayed with the 🛡 icon.

4. In the opened prompt window, confirm deletion of the report templates.

Deleting a report

Only users with the Administrator role can delete reports in the application.

To delete a report:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select one or more reports that you want to delete.

   Reports in the reports table are filtered based on the IDs of reports that were last run in the current Server connection session. To display all generated reports, reset the filter settings by clicking the **Default filter** button. If necessary, you can configure filtering based on a specific period of time.

   The details area appears in the right part of the web interface window.
3. Click the **Delete** button.
4. In the opened prompt window, confirm deletion of the report.

Canceling report generation

You can cancel report generation only for a report with the *In progress* status.

If necessary, a user with the Administrator role can cancel generation of reports started by any user of the application.

To cancel generation of a report:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select the report with the *In progress* status that you want to cancel.

   The details area appears in the right part of the web interface window.
3. Click the **Cancel** button.
4. In the opened prompt window, confirm cancellation of report generation.

After this request is fulfilled, the report status changes to *Canceled*.

Managing the settings for storing report files

You can change the limits on the maximum space used for storing report files.

To edit the report file storage settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the Server tile.

   The details area appears in the right part of the web interface window.
4. Click the **Edit** button.

   The details area will show the tabs for configuring the Server parameters.

5. On the **General** tab go to the **Reports** settings group and use the **Space** setting to define a limit for the space used to store report files.

   You can select the unit of measure for the space limit: **MB** or **GB**.

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for report files, and specify the minimum number of days.

7. Click **Save**.

Managing a security policy

A *security policy* is a set of data that defines the following operational settings of the application:

- User-defined sets of Intrusion Detection rules
- Allow rules for Interaction Control and for events
- Settings of devices and tags that are used for Asset Management and Process Control
- Network map display settings
- Address space settings
- Event types settings
- Risk types settings

All other application settings are not part of a security policy and are applied separately from it. This includes the settings of nodes that have components installed, the list of application users, objects linking events and devices in the devices table, and other settings.

A security policy is stored on the Server and is automatically updated each time application settings are modified (for example, when Interaction Control rules are added).

You can export a security policy to files and import them from files. You can also clear the current security policy on the Server to delete all previously saved settings.

When exporting, importing or clearing a security policy, you can select specific sections of the policy that you want to export, import, or clear. For example, you can export only devices and allow rules.

When exporting a security policy, the application creates a file containing information about the selected application settings. To import settings, you can select a previously exported file.

Changing the contents of a security policy file may result in a malfunction of Kaspersky Industrial CyberSecurity for Networks if you import a security policy from this modified file. The application may stop performing protection functions for the industrial network.

Exporting a security policy to a file

The settings that are part of a security policy can be exported to a file. You can export the entire security policy or its individual sections.

When necessary, you can then import the relevant application settings from the file containing the saved security policy.

To export the current security policy:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Security policy**.
3. Click the **Export** button.

   You will see the security policy tree in which you can select the necessary sections to export.
4. Select the check boxes for the relevant sections of the security policy.
5. Click the **Export** button.
6. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Importing a security policy from a file

You can import application settings from a file containing a saved security policy. For this kind of import, you can use a file that was obtained when exporting a security policy.

When importing security policy sections, the application first clears the current contents of these sections and then imports data into these sections.

If a file contains multiple sections of a security policy, you can select the relevant sections to import.

> A security policy cannot be imported if updates are currently being installed or if another import process is running.

Only users with the Administrator role can import a security policy from a file.

To import a security policy from a file:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Security policy**.

3. Click the **Import** button.

   This opens the standard browser window for selecting a file.

4. Specify the path to the security policy file.

5. Click the button for opening the file.

   After the file contents are checked, you will see a security policy tree showing the sections that can be imported.

6. Select the check boxes for the security policy sections that you want to import into the application.

7. Click the **Import** button.

The security policy import process begins. The application Server is unavailable for connections until the import process is complete. During the import process, the application web interface page displays a special section named **Application maintenance**.

Clearing the current security policy

You can clear the current settings that are part of a security policy. This can be done for the entire security policy or for some of its individual sections.

After a security policy is cleared, it will be impossible to recover some of its data even if you exported the security policy in advance. For example, after you clear a section containing device information, all the objects linking events and devices in the devices table are permanently deleted.

A security policy cannot be cleared if updates are currently being installed or if the data import process is running.

Only users with the Administrator role can clear a security policy.

To clear a security policy:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select **Settings** → **Security policy**.

3. Click the **Clear** button.

   You will see the security policy tree in which you can select the relevant sections to clear.

4. Select the check boxes of the security policy sections that you want to clear.

5. Click the **Clear** button.

The security policy clearing process begins. The Application Server is unavailable for connections until the clearing process is complete. During the clearing process, the application web interface page displays a special section named **Application maintenance**.

Converting a security policy from a previous version of the application

If you want to import a file containing a saved security policy from a previous version of the application into the current version of the application, you need to convert this file by using the policy_updater.py policy conversation script. This script is located on the Server computer in the /opt/kaspersky/kics4net/sbin/ folder.

The policy_updater.py script is designed for converting security policies exported to Kaspersky Industrial CyberSecurity for Networks 3.1 and later.

To convert a file containing a security policy that was created in the previous version of the application:

1. Open the operating system console on the Server computer and go to the /opt/kaspersky/kics4net/sbin/ folder.

2. Enter the following command in the command line:

   ```
   python3 ./policy_updater.py -i <path to the file of the original policy> -o <path to the file of the converted policy>
   ```

   Example:

   ```
   python3 ./policy_updater.py -i /home/user1/policy_2023-09-01_12-00 -o /home/user1/policy_for_4_1
   ```

The obtained file can be imported into the current version of the application.

Using the Kaspersky Industrial CyberSecurity for Networks API

Kaspersky Industrial CyberSecurity for Networks has an application programming interface (API) that provides access to application functions for external applications (hereinafter referred to as "recipient apps").

The Kaspersky Industrial CyberSecurity for Networks distribution kit includes a package containing descriptions of specifications for representing data in requests sent to the REST API server. The *REST API server* runs on the Kaspersky Industrial CyberSecurity for Networks Server computer and processes requests by using the architectural style of interaction known as REST (Representational State Transfer). Queries to the REST API server are sent over the HTTPS protocol. You can configure the REST API server settings under **Settings** → **Connection Servers** (including to replace the default self-signed certificate with a trusted certificate).

The JSON format is used to represent data in requests and responses.

The documentation containing descriptions of requests based on the REST architectural style is published as an Online Help Guide on the Kaspersky Online Help page. This documentation serves as the Developer Guide. The Developer Guide also provides sample code and detailed descriptions of called elements that are available in requests sent to the REST API server.

OPEN THE DOCUMENTATION DESCRIBING REQUESTS TO THE REST API SERVER, version 3

OPEN THE DOCUMENTATION DESCRIBING REQUESTS TO THE REST API SERVER, version 4

Recipient apps can use the Kaspersky Industrial CyberSecurity for Networks API to do the following:

- Receive data on devices known to the application.
- Add, modify, and delete devices.
- Receive data on registered events.
- Send events to Kaspersky Industrial CyberSecurity for Networks (the system event type with code 4000005400 is used for registering the events).
- Receive data on tags and tag parameters.
- Subscribe to notifications about received tag values.
- Receive data on detected vulnerabilities.
- Receive application messages and audit entries.
- Receive data on allow rules.
- Enable, disable, and delete allow rules.
- Receive data on risks associated with devices.
- Receive data on address spaces.
- Send a report on the network topology map to Kaspersky Industrial CyberSecurity for Networks.
- Receive the following application data:
  - List of nodes that have application components installed

- List of monitoring points and their parameters
- List of supported protocol stacks and their parameters
- List of event types and their parameters
- Current state and operating mode of technologies
- Application version and release dates of the installed updates
- Information about an added license key
- Application localization language

All of the listed actions are available when making requests to the REST API server version 4. Some of these actions are not supported when making requests to the REST API server version 3.

Recipient apps that utilize the Kaspersky Industrial CyberSecurity for Networks API can connect to the Application Server through connectors. Connectors use certificates for a secure connection. For each recipient app that will send requests to the REST API server, you need to create a separate connector in Kaspersky Industrial CyberSecurity for Networks.

A recipient app must use an authentication token for a connection with Kaspersky Industrial CyberSecurity for Networks. The application issues an authentication token upon request by the recipient app, and for this token it uses certificates of the connector that was created for this recipient app. An authentication token is valid for 10 hours. The recipient app can renew the authentication token by special request.

Documentation containing a description of queries for authentication token operations is published as an Online Help Guide on the Kaspersky Online Help page. This documentation serves as the Developer Guide.

OPEN THE DOCUMENTATION DESCRIBING QUERIES FOR AUTHENTICATION TOKEN OPERATIONS, version 3

OPEN THE DOCUMENTATION DESCRIBING QUERIES FOR AUTHENTICATION TOKEN OPERATIONS, version 4

The Kaspersky Industrial CyberSecurity for Networks API provides the following options for working with recipient apps:

- Interaction based on the REST architectural style
- Interaction over the WebSocket protocol

Recipient apps can use the WebSocket protocol for interaction in the Kaspersky Industrial CyberSecurity for Networks API to create subscriptions to modified values received by the application. For example, this method of interaction lets you subscribe to notifications about the received values of a specific tag.

Securing interactions when using the Kaspersky Industrial CyberSecurity for Networks API

Recipient apps obtain access to application functions by using the Kaspersky Industrial CyberSecurity for Networks API after establishing encrypted connections over the HTTPS protocol. Connections are secured by using certificates issued by the Kaspersky Industrial CyberSecurity for Networks Server. The Server issues certificates for the connectors that are used by recipient apps to connect to the Server.

A separate certificate must be created for each recipient app. A connection can be established through a connector only by using the specific certificate that was issued by the Server and saved in the communication data package for that connector. A connection cannot be established if a recipient app uses a certificate from a different connector or different Kaspersky Industrial CyberSecurity for Networks Server, or a certificate that is used for other connections (such as a sensor certificate).

After establishing an encrypted connection, the recipient app must request an *authentication token* for the connector that will be indicated by the recipient app in requests sent to the REST API server. Before issuing an authentication token, the Server verifies the current state of the application user account that was indicated when the connector was created. The Server will not issue an authentication token if the application user account has been deleted or blocked.

An authentication token is valid for a period of 10 hours after it was issued by the Server. If a token needs to be used for a longer period, the recipient app must request a time extension before the token expires.

> For information on the requests and methods provided in the Kaspersky Industrial CyberSecurity for Networks Server API, please refer to the documentation for the Kaspersky Industrial CyberSecurity for Networks API.

When the Server receives requests from the recipient app during the validity period of the authentication token, the Server verifies the existence and current access rights of the application user account that was indicated when the connector was created. A method indicated in a request from a recipient app is not executed if the user account is not found (has been deleted from the application), or if the user account does not have sufficient rights to perform the operation (the user account role does not match the performed operation).

When processing requests from recipient apps, the application uses the audit log to store information about attempts to perform the following operations:

- Receive an authentication token.
- Extend the validity period for an authentication token.
- Add a device to the devices table.
- Edit device information.
- Delete a device.
- Query the audit log (when first reading audit entries through the connector after loading the web server).

Creating and using connectors for the Kaspersky Industrial CyberSecurity for Networks API

To enable a recipient app to interact with the application by using the Kaspersky Industrial CyberSecurity for Networks API, you need to add a connector for this app. When creating a connector, you must indicate the **Generic** system type for the connector.

When adding a connector and when creating a new communication data package for this connector, the Server generates a communication data package that you need to use for the connector to work.

A communication data package is an archive containing the following files:

- certificates.pfx – encrypted file containing the Server's public certificate key and the certificate issued by the Server for the connector (with the private key). The contents of the file are encrypted with the password that was set when the connector was added or when a new communication data package was created for this connector.
- metadata.json – contains the configuration data for the connector. Data is represented in JSON format.

The listed files must be used to connect a recipient app through the connector. To decrypt the certificates.pfx file and apply the certificate and keys within it, you can use the standard methods for handling files of this format (for example, `openssl` commands). The addresses indicated in the metadata.json file are required for the connector to work and for sending requests to the REST API server.

The certificate and configuration data in the communication data package are valid until a new communication data package is created or until the connector is removed from the application.

Subscribing to notifications about tag values over the WebSocket protocol

When using the Kaspersky Industrial CyberSecurity for Networks API, a recipient app can create a subscription to notifications regarding modified values of a specific tag. The WebSocket protocol is used for creating a subscription and receiving notifications.

A subscription for a recipient app consists of the following steps:

1. **The recipient app establishes a connection with the Kaspersky Industrial CyberSecurity for Networks Server through the connector for this application using the REST API server.**

   After successfully connecting to the Server, the connector receives an authentication token. The connector uses the authentication token for all subsequent interactions with the Server in this session (specifically, for requesting its configuration from the Server).

2. **The recipient app uses WebSocket to connect and sends a request to create a subscription to notifications regarding the received values of a relevant tag.**

   The Kaspersky Industrial CyberSecurity for Networks Server receives the request and creates the subscription. A request is sent by using the appropriate functions provided by the WebSocket protocol.

3. **Kaspersky Industrial CyberSecurity for Networks detects a new tag value in traffic when reading or writing a tag.**

4. **Kaspersky Industrial CyberSecurity for Networks sends the obtained tag value to the recipient app that has an active subscription to notifications regarding the values of this tag.**

Main features of a subscription:

- After the recipient app indicates the relevant tags of Kaspersky Industrial CyberSecurity for Networks, the Server sends confirmation regarding the capability to obtain the values of those tags. The recipient app then waits to receive the values of those tags over the established connection.
- Creation and maintenance of a subscription relies on the WebSocket protocol and a connection at the same address that is used by the REST API server.

- A Kaspersky Industrial CyberSecurity for Networks Server supports no more than one active subscription for tag values. If an active subscription was already created and is being used, and you attempt to create another subscription, you will see an error regarding an excessive number of connections.

- The recipient app has the capability to close an established connection for a subscription at any time to stop receiving tag values.

- A subscription is stopped if it is intentionally closed by the recipient app or if the connection is disrupted. If the Kaspersky Industrial CyberSecurity for Networks Server was temporarily unavailable (disconnected) and tag values were not forwarded for the subscription, the recipient app must re-subscribe to the tag values after the connection is restored.

Connecting with WebSocket

To receive tags by subscription, you can use the standard functions of WebSocket as well as the SignalR Core library. Packages for working with the SignalR Core library are available for the most common programming languages: C++, C#, Java, Python, Go, and JavaScript/TypeScript.

To connect using WebSocket, you need to specify the following address:
`<publicApi address from the communication data package>/kics4net/api/v4/tag-values`

However, the protocol indicated in the address string depends on the functionality utilized for the connection.

If the SignalR Core library is being used, the address string begins with `https://`. For example:
`https://kics-server:8080/kics4net/api/v4/tag-values`

If the standard functions of WebSocket are being used, you need to replace `https` with `wss` in the address string. For example:
`wss://kics-server:8080/kics4net/api/v4/tag-values`

If an authentication token is not provided when connecting (or the provided token has not passed verification), the server returns code 401 when responding to a request to open the connection.

Creating a subscription for tag values

To create a subscription, you must make a request with the `GetTagValuesStream` method name.

Example request argument:

```
{
 "tagIdentifiers": [
 { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
 { "tagName": "Asdu_1_object_1003", "assetName": "Asset 079" }
 ],
 "streamConfig": {
 "samplingRateHz": 1
 }
}
```

A request argument consists of the following fields:

- `tagIdentifiers` – array of IDs of tags whose values need to be received for the subscription.

- `assetName`, `tagName` – values representing the device name and tag name (used to identify the tag whose values are needed for the subscription).

- `samplingRateHz` – tag value sampling rate (used to reduce the volume of transmitted data). If a null value is defined for the field, sampling is not performed.

If a subscription creation argument does not satisfy the requirements of the fields, an error is returned with a description of the problem.

Example error for a subscription creation argument:

```
HubException: GetTagValuesStreamRequest has validation errors:
 TagIdentifiers:
 The TagName field is required.
 The StreamConfig field is required.
```

Confirming a subscription

When confirming a subscription, the server returns a confirmation result for each tag that matches a `tagIdentifiers` value in the request.

Example subscription confirmation:

```
{
 "confirmation": {
 "result": "ok",
 "tagIdentifier": { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
 "tagId": 102
 }
}
```

A response containing a subscription confirmation consists of the following fields:

- `result` – status of the tag value subscription. Possible values:
  - `ok` – subscription was successfully created.
  - `notFound` – a tag with the specified `assetName` or `tagName` was not found.
- `tagIdentifier` – tag ID equivalent to one value from the `tagIdentifiers` array of arguments of a subscription creation request.
- `tagId` – unique ID of a tag in the application. This can be used to receive information about a tag through the Kaspersky Industrial CyberSecurity for Networks API, or to identify a tag in a response containing its values.

Tag values by subscription

The application sends tag values by subscription within a fields structure. The following fields are presented at the top level of the structure:

```
{
 "value": {
 "tagId": <unique ID of the tag in the application>,
 "tagValue": "<JSON object with tag data>"
 }
}
```

Information about a new value of a tag is sent to the recipient app in JSON format. The sent data object contains the following fields:

- `n` – tag data type represented by the name from `TagStructure`.
- `ts` – time when the last update of tag values was registered. Indicated in microseconds starting on 01/01/1970.
- `dn` – transfer direction. Possible values: `r`, `w`, `rw`.

- `mp` – monitoring point ID.
- `d` – contents of tag fields.

The `d` attribute represents a dictionary in which each key is the name of a null-hierarchy tag field. Each field value has the following attributes:

- `t` – mandatory attribute indicating one of the following data types:
  - `u` – UINT64.
  - `i` – INT64.
  - `b` – BOOL.
  - `d` – DOUBLE.
  - `s` – UTF8 string.
  - `t` – time in microseconds starting on 01/01/1970.
  - `e` – ENUM. The field additionally contains the following attributes:
    - `n` – name of the ENUM type.
    - v – original value of ENUM.
    - s – string value of ENUM.
  - `st` – structure.
  - `un` – UNION.
- `v` – mandatory attribute indicating the tag field value.
- `n` – name of the ENUM type from `TagStructure` (only for the `e` type – ENUM).
- `s` – string value of ENUM (only for the `e` type – ENUM).

  Example:

  ```
  - enum:
  name: OpType # Name of ENUM type ('n' attribute)
  data:
  0: NUL # 0 is written to the 'v' attribute, NUL is written to the 's' attribute
  1: PULSE_ON
  2: PULSE_OFF
  ```

- `x` – identifies the main value of the tag.

  Format: `"x": 1`

  The `x` attribute is absent from all other fields of the tag.

- m – special marker of the tag parameter. This corresponds to the marker attribute with the following fields:

- `q` – value of the quality attribute.
- `ts` – timestamp status displaying its accuracy, temporary state, or reason for an error during verification.
- `ds` – data status.
- `o` – origin of the value or command.
- `t` – time when the tag values were last updated (taken from traffic).
- `ct` – cause of transmission.

Format: `"m": "q"`

Example of a forwarded tag value in JSON format:

```
{
 "n": "TagStructure1",
 "ts": 18446744073709551616,
 "dn": "r",
 "mp": 1,
 "d":
 {
 "value":
 {
 "t": "d",
 "v": 3.1415,
 "x": 1
 },
 "quality":
 {
 "t": "s",
 "v": "good",
 "m": "q"
 },
 "mask":
 {
 "t": "u",
 "v": 18446744073709551616
 },
 "enumfield":
 {
 "t": "e",
 "n": "SwitchState",
 "v": 0,
 "s": "Off"
 },
 "strucfield":
 {
 "t": "st",
 "v":
 {
 "v1":
 {
 "t": "d",
 "v": 3.1415
 },
 "q2":
 {
 "t": "s",
 "v": "good",
 "m": "q"
 }
 }
 },
 "unionfield":
 {
 "t": "un",
 "v":
 {
 "_":
 {
 "t": "u",
 "v": 42
 },
 "low4bits":
 {
 "t": "u",
 "v": 10
 },
 "high4bits":
 {
 "t": "u",
 "v": 2
 }
 }
 }
 }
}
```

Examples of receiving tag values by subscription

Below is an example of receiving tag values by subscription using standard WebSocket functions in Python.

You must first run the following command:
`pip install websocket_client`

Example subscription using standard WebSocket functions:

```
import json, ssl, websocket


def on_message(ws, message):
 print(message)


def on_error(ws, error):
 print(f' error: {error}')


def on_close(ws):
 print("### closed ###")


def on_open(ws):
 print("connection opened and handshake received ready to send messages")

 # all sent messages must end with this character
 message_separator = chr(30)

 # setting up json as messages format
 protocol_selection_args = {
 'protocol': 'json',
 'version': 1
 }
 ws.send(json.dumps(protocol_selection_args) + message_separator)

 # creating subscription
 args = {
 'arguments': [
 {
 'tagIdentifiers': [
 {
 'tagName': 'tag_01',
 'assetName': 'asset_02'
 }
 ],
 'streamConfig': {
 'samplingRateHz': 5
 }
 }
 ],
 'invocationId': '0', # will be included in response message
 'target': 'getTagValuesStream',
 'type': 4 # must be equal to 4 for outgoing messages
 }

 ws.send(json.dumps(args) + message_separator)


 def login():
 token = "you should get access token for API here"
 return token


if __name__ == "__main__":
 server_url = "wss://localhost:8091/kics4net/api/tag-values"
 auth = "Authorization: Bearer " + login()

 # for troubleshooting uncomment next line
 # websocket.enableTrace(True)
 ws = websocket.WebSocketApp(server_url,
 on_message=on_message,
 on_error=on_error,
 on_close=on_close,
 header=[auth])

 print(f'opening connection to {server_url}')
 ws.on_open = on_open
 ws.run_forever(
 # use it only if Server has self-signed certificate
 sslopt={"cert_reqs": ssl.CERT_NONE}
 )
```

Below is an example of receiving tag values by subscription using the SignalR Core library in Python.

You must first run the following command:
`pip install signalrcore`

Example subscription using the SignalR Core library:

```
import logging
from signalrcore.hub_connection_builder import HubConnectionBuilder

TOKEN = 'you should get access token for API here'
IP = '192.168.0.7'
PORT = '8080'
HUB = 'kics4net/api/v4/tag-values'
```

```
class WebsocketConnection(HubConnectionBuilder):
 def __init__(self, url: str = None, options: dict = None, verify_ssl: bool = False):
 super().__init__()
 self.with_url(url, options=options)
 self.configure_logging(logging.WARNING)
 self.with_automatic_reconnect({
 "type": "raw",
 "keep_alive_interval": 10,
 "reconnect_interval": 5,
 "max_attempts": 5
 })
 self.verify_ssl = verify_ssl

 def on_tag_stream_value(self, m):
 result.append(m)
 print(f'on_new_tag_value, {m}')

 def on_tag_strean_error(self, e):
 print(f'onError, {e}')

 def on_tag_stream_complete(self, q):
 print(f'onComplete, {q}')

 def subscribe_tags(self):
 print("connection opened and handshake received ready to send messages")

 args = {
 'tagIdentifiers': [
 {
 'tagName': 'tag_01',
 'assetName': 'asset_02'}
 ],
 'streamConfig': {
 'samplingRateHz': 5
 }
 }

 self.stream("GetTagValuesStream", [args]) \
 .subscribe({
 "next": self.on_tag_stream_value,
 "complete": self.on_tag_stream_complete,
 "error": self.on_tag_strean_error
 })

def main():
 server_url = "https://{}:{}/{}".format(IP, PORT, HUB)
 login = 'bearer {}'.format(TOKEN)

 conn = WebsocketConnection(url=server_url, options={"headers": {"authorization": login}})
 conn.build()

 logging.info(f'opening connection to {server_url}')
 conn.on_open(conn.subscribe_tags)
 conn.start()

 logging.info('closing connection')
 conn.stop()


if __name__ == '__main__':
 main()
```

Performing common tasks

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

System monitoring in online mode

Kaspersky Industrial CyberSecurity for Networks displays data for monitoring the current state of the system in the **Dashboard** section of the application web interface. Data is automatically updated in online mode.

Data in the **Dashboard** section is presented as individual blocks called *widgets*. Depending on its purpose, a widget may contain an updatable value or message about the current state of the application, or provide expanded information about up-to-date data.

The **Dashboard** section may display the following widgets:

- Widgets containing information for monitoring the current state of the system and the most significant changes:
  - **Devices and security states** – distribution of devices by their security state.
  - **Event scores** – histogram that arranges events based on their scores for the selected period. Columns of the histogram correspond to integer values of event scores. You can change how data is displayed on the pie chart that arranges events by their severity level. Depending on the numerical value of its score, an event may have a severity of *Low* (score of 0.0–3.9), *Medium* (4.0–7.9) or *High* (8.0–10.0).
  - **Events by technology** – shows the quantitative distribution of events based on the various event registration technologies for the selected period.
  - **Frequently encountered users of applications in events** – shows the most frequently registered user names in events based on data from EPP applications for the selected period.
  - **Frequently encountered users of applications in events** – shows the most frequently registered user names in events based on data from EPP applications for the selected period.
  - **Frequently encountered devices in events** – shows the most frequently registered devices in events for the selected period.
  - **Top devices by risk count** – shows the most frequently registered devices in detected risks for the selected period.
  - **Risk scores** – histogram that arranges risks based on their scores for the selected period. Columns of the histogram correspond to integer values of event scores. You can change how data is displayed on the pie chart that arranges risks by their severity level. Depending on the numerical value of its score, a risk may have a severity of *Low* (score of 0.0–3.9), *Medium* (4.0–7.9) or *High* (8.0–10.0).
  - **Situational awareness** – shows notifications about currently identified threats to system security (for example, **Detected 10 unauthorized network interactions**). This widget displays notifications in the order of their severity.
  - **Protection by EPP applications** – quantitative ratio of computers protected by EPP applications to computers not protected by EPP applications. The center of the pie chart displays the total number of protected and unprotected computers.

    A computer is considered to be protected by an EPP application if Kaspersky Industrial CyberSecurity for Networks has information regarding fulfillment of the following conditions:

    - An EPP application is installed on the computer.

    - The Real-Time Protection task is being performed for the EPP application.

    - The EPP application has an Active *connection to the integration server*.

    A computer is considered to be unprotected by an EPP application if at least one of the listed conditions is not fulfilled. The EPP application protection check is performed for all devices in Kaspersky Industrial CyberSecurity for Networks containing the name of a Windows operating system (any version) as the installed operating system, or if devices belong to one of the following categories:

    - **Server**

    - **Workstation**

  - **Devices** – contains information about devices in the industrial network (arranged by device category).

  - **Events** – contains information about the events and incidents that have the most recent values for the date and time of last occurrence.

- Widgets containing information about the application and about the hardware resources of the Server and sensors:

  - **Traffic** – rate of incoming traffic. This widget can display data on all monitoring points of all nodes that have application components installed, data on monitoring points of the selected node, or data on one individual monitoring point.

  - **Processor** – processor utilization on the selected node that has an application component installed.

  - **RAM** – amount of physical RAM being used on the selected node that has an application component installed.

  - **Performance** – information about the current state of application performance. This widget can display the following values:

    - **OK** – there are no messages regarding performance issues, or all performance issues have been resolved.

    - **Non-critical malfunction** – there are messages regarding non-critical malfunctions (this is displayed until the performance issue is resolved).

    - **Operation disrupted** – there are messages regarding application performance issues (this is displayed until the performance issue is resolved).

    - **Maintenance mode** – the application is running in maintenance mode.

  - **Tags** – rate of processing of tags detected by the application. This widget can display data on all monitoring points of all nodes that have application components installed, data on monitoring points of the selected node, or data on one individual monitoring point.

  - **Storage** – information about the drive in the local file system on the selected node with the application component installed. On this widget, you can select the following data to be displayed:

    - **Disk usage** – percentage of time taken to process data read/write operations.

    - **Occupied on disk** – volume of used disk space.

        - **Read from disk** – rate of reading data from the disk.

        - **Write to disk** – rate of writing data to the disk.

    - **Traffic processing latency** – current delay in traffic processing from the time it arrives at a monitoring point of the node (displays the maximum delay time received from all enabled monitoring points). This widget can display data on all monitoring points of all nodes that have application components installed, or data on monitoring points of the selected node.

    - **Status of functions** – general information about the current state of protection functions in the application. This widget can display the following values:

        - **All are enabled** – all technologies and methods designed for continual use are enabled, and all created monitoring points are enabled.

        - **Not all are enabled** – some protection functions are disabled or are enabled in learning mode, or not all monitoring points are enabled.

    - **Uptime** – operating time of Kaspersky Industrial CyberSecurity for Networks. On this widget, you can select the following data to be displayed:

        - **Effective uptime** – duration of normal operation of the application (without malfunctions) since the most recent startup until the current moment.

        - **Total uptime** – operating time since the first startup of the application until the current time (includes periods of normal operation and periods when the application was running with malfunctions).

        - **Since first start of application** – total time that has elapsed since the first startup of the application until the current time (includes periods of normal operation, periods when the application was running with malfunctions, and periods when the application was not operational).

- Widgets without dynamically updated information. You can create widgets with user-defined contents. These widgets are called *custom* widgets. For example, you can use custom widgets to logically separate groups of widgets in the **Dashboard** section.

Widgets provide various ways to get your attention depending on incoming data. For example, widgets containing information about the application and hardware resources can automatically change color if the information requires attention (for instance, when the load on a hardware resource is nearing critical load).

Widgets display only the main information, which is dynamically updated. If you need to view more detailed information (for example, about devices with issues), you can proceed from the **Dashboard** section to other sections of the application web interface. You can switch between sections by using your mouse to select interface elements of widgets.

Adding a widget

To add a widget:

1. In the **Dashboard** section, click the **Widgets** button.

   The **Add widgets** window opens.

2. Add the necessary widget by clicking the **Add** link on the right of the widget name.

   The new widget will occupy the free space in the widget display area.

3. Click the **Close** button in the **Add widgets** window.

After adding a widget, you can configure how the widget is displayed.

Configuring how widgets are displayed

You can use the following functions to configure how widgets are displayed:

- **Moving a widget**

  1. In the **Dashboard** section, move your cursor over the upper part of the relevant widget (for example, over the widget name).

     The cursor will change to ✥.

  2. Drag the widget to the appropriate part of the widget display area.

- **Changing the size of a widget**

  1. In the **Dashboard** section, move your cursor over the lower-right corner of the relevant widget.

  2. Click and hold the left mouse button to set the size for the widget border.

- **Changing the settings for displaying data in a widget**

After a widget is added, the default settings are used to display data in the widget. You can change the display settings if necessary (for example, to indicate the relevant source or to select other data to display in the **Storage** widget).

To configure the widget display settings:

1. In the **Dashboard** section, use the ⚙ button in the upper-right corner of the widget to open the widget management window.
2. In the widget management menu, select the **Configure** option.

   This opens the window for configuring the display settings.
3. Configure the widget settings.

   Depending on the selected widget, the window may contain the following settings:

   - **Change name** – if the **Change name** check box is selected, you can define any name for the widget (different from the default name) in the **Widget name** field. The **Change name** setting is absent from custom widgets.
   - **Widget name** – field for entering a widget name different from the default name.
   - **Edit description** – if the **Edit description** check box is selected, you can provide any description for the widget (different from the default description) in the **Widget description** field. The **Edit description** setting is absent from custom widgets.
   - **Widget description** – field for entering a widget name different from the default name.
   - **Refresh period** – defines how frequently the displayed data is refreshed (time interval in seconds).
   - **Display** – defines the type of displayed data (for widgets that let you select which data to display).
   - **Data source** – defines the node with installed application components whose data is displayed in the widget. If the **Entire application** option is selected, the widget displays data from all nodes.
   - **Monitoring point** – defines the monitoring point of the selected node for displaying data. If the **All monitoring points** option is selected, the widget displays data for all monitoring points of the selected node.
   - **Change color based on status** – if this check box is selected, the background color of the widget automatically changes depending on the severity of the incoming data. A red background signifies critical (maximum) severity of data. If this check box is cleared, background coloring is disabled.
   - **Defined background** – defines the color of the background on the custom widget. You can choose a background color that corresponds to one of the severity levels (**Info**, **Warning**, **Critical**), or use the **Neutral** option to disable background coloring.
   - **Display mode** – determines how data is displayed in the widget. You can configure the widget to display data as a histogram or pie chart.
   - **Take into account events with Resolved status** – if the **Take into account events with Resolved status** check box is selected, the widget displays data for all events.
   - **Include remediated and accepted risks** – if the **Include remediated and accepted risks** check box is selected, the widget displays data for all risks.
4. Click **OK**.

Information in the Devices widget

The **Devices** widget in the **Dashboard** section displays information about devices that are included in the list of known devices.

The widget provides the following information:

- Data on the number of devices known to the application in each category. This data is displayed as category icons in the upper part of the widget. The number of devices of the specific category is indicated under the icon of each category. If the list of devices contains devices with issues, the warning icon is displayed on the category icons of these devices.
- List of categories with devices with issues. This data is displayed in the middle part of the widget if such devices are present. The space used for displaying graphical elements is limited by the size of the widget.

Devices with issues

The application determines that a device requires attention in any of the following cases:

- The device has the *Authorized* status and a security state other than *OK*.
- The device has the *Unauthorized* status.

If there are devices with issues, the following information is displayed for each category in the list:

- Line containing the category icon, text comment, and link containing the number of devices with issues.
- Line containing the graphical elements representing the devices. This line is displayed if there is sufficient free space in the widget. The number of graphical elements in the line depends on the current size of the browser window. If there are more devices with issues than the number of graphical elements displayed in the line, the number of hidden devices is displayed on the right in the format `+<number of devices>`.

Graphical elements of devices

Graphical elements representing devices contain the following information:

- Device name.
- Device status. This is displayed as an icon if the device has the *Unauthorized* status.
- Device security state. This is displayed as a colored line on the left border of the graphical element. The color of the line corresponds to the *OK*, *Warning* or *Critical* states.

The graphical elements are displayed in the following order:

1. Devices assigned the *Unauthorized* status.
2. Devices with the *Critical* security state.
3. Devices with the *Warning* security state.

Navigating to other sections from the **Devices** widget

You can use elements of the **Devices** widget interface to navigate to the devices table and display detailed information about devices. To do so, you can utilize the following options:

- Go to the devices table and filter the table ?

  To go to the devices table and view information about all devices in the selected category:

  In the upper part of the **Devices** widget, click the icon of the relevant category.

  This opens the **Devices** section containing the devices table. The table will be filtered based on the selected category of devices.

  To proceed to the devices table and view information about devices with issues that belong to a specific category:

  In the list of categories containing devices with issues, click the link displaying the number of devices in the relevant category. This link is displayed at the end of the line with the category icon and text comment **with issues**.

  This opens the **Devices** section containing the devices table. The table will be filtered based on the IDs of devices with issues that belong to the specific category.

  > The devices table is filtered based on the IDs of those devices that were displayed in the **Devices** widget when you proceeded to the devices table. After you switch to the devices table, the filter settings are not updated. If you want to view the current number of devices with issues, you can go to the **Dashboard** section again.

  To go to the devices table and view information about a device with issues:

  In the **Devices** widget, click the graphical element that represents the relevant device.

  This opens the **Devices** section containing the devices table. The table will be filtered based on the device ID.

  To go to the devices table without changing the current table filter settings:

  Click the **Show all devices** link in the **Devices** widget.

  This opens the **Devices** section containing the devices table. The table will display the devices that satisfy the filter settings that were previously defined in the devices table.

- Go to the devices table and search the table ?

  1. In the **Devices** widget, enter your search query into the **Search devices** field.
  2. Click the **Search** button.

  This opens the **Devices** section containing the devices table. The table will display the devices that meet the search criteria.

Information in the Events widget

The **Events** widget in the **Dashboard** section displays general information about the events and incidents that have the most recent values for the date and time of last occurrence.

The widget displays the following elements:

- Histogram of events and incidents for the selected period. This data is displayed in the upper part of the widget. The histogram shows the distribution of events and incidents based on their severity levels.

- List containing information about registered events and incidents sorted by date and time of last occurrence. This data is displayed in the middle part of the widget.

Statistics of events and incidents

On the histogram showing the distribution of events and incidents, the columns correspond to the total number of events for each time interval. Within columns, the severities of events and incidents are distinguished by color. The following colors correspond to severity levels:

- Blue. This color is used for events and incidents with the *Low* severity level.

- Yellow. This color is used for events and incidents with the *Medium* severity level.

- Red. This color is used for events and incidents with the *High* severity level.

To display information about a column of the histogram, move the mouse cursor over it. A pop-up window shows the date and time of the interval as well as the number of events and incidents by severity level.

The duration of time intervals depends on the selected display period. You can select the relevant period for generating a histogram using the following buttons:

- **1h**—period of one hour, divided into intervals of one minute.

- **12h**—period of 12 hours, divided into one-hour intervals.

- **24h**—period of 24 hours, divided into one-hour intervals.

- **7d**—period of seven days, divided into intervals of one day.

List of events and incidents

The list of events and incidents in the **Events** widget is updated in online mode. Events and incidents with the most recent values for the date and time of last occurrence are placed at the beginning of the list.

The number of displayed elements in the list of events and incidents is limited by the size of the widget.

The following information is provided for each event or incident in the list:

- Title of the event or incident.

- Date and time of last occurrence.

- Icon designating the severity level of an event or incident:
  - ⓘ – *Low* severity.
  - ⚠ – *Medium* severity.
  - ❗ – *High* severity.

Incidents in the list are marked with the 📁 icon.

Navigating to other sections from the **Events** widget

You can use elements of the **Events** widget interface to go to the events table and display detailed information about events and incidents. To do so, you can utilize the following options:

- Go to the events table and filter the table ⍰

  You can view detailed information about an event or incident by clicking the relevant event or incident in the **Events** widget list. Doing so will open the **Events** section in which the table will be filtered based on the ID of the selected event or incident. The period ranging from the date and time of registration of the event or incident to the current moment (without indicating an end boundary for the period) will also be defined for the filter.

  If you want to proceed to the events table without changing the current table filter settings in the **Events** section, click the **Show all events** link in the **Events** widget.

- Go to the events table and search the table ⍰

  1. In the **Events** widget, enter your search query into the **Search events** field.
  2. Click the **Search** button.

     The **Events** section opens. The events table displays the events and incidents that meet the search criteria.

Removing a widget

To remove a widget:

1. In the **Dashboard** section, use the ⚙ button in the upper-right corner of the widget to open the widget management window.
2. In the widget management menu, select the **Remove** option.

   A window with a confirmation prompt opens.
3. In the prompt window, confirm removal of the selected widget.

Asset Management

Kaspersky Industrial CyberSecurity for Networks lets you monitor industrial network devices that are considered to be company assets. To manage these assets, you can view the devices table in the **Assets** section of the Kaspersky Industrial CyberSecurity for Networks web interface. You can also view information about the interactions between devices and perform various actions with devices when working with the network interactions map and with the topology map.

Devices table

A devices table is created for the purpose of asset management in the application. All devices in the table are considered to be known to the application. You can view the devices table in the **Assets** section on the **Devices** tab.

The devices table has the following limitations on the number of elements:

- The total number of devices with the *Authorized* and *Unauthorized* statuses can be no more than 100 thousand.

  If the maximum number of devices with the *Authorized* or *Unauthorized* statuses is reached, new devices with these statuses are not added to the table. If this is the case, to add a new device to the table you need to remove one of the previously added devices.

- The number of devices with the *Archived* status can be no more than 100 thousand.

  If the maximum number of devices with the *Archived* status is reached, new devices with this status are added to the table in place of devices that have went the longest without showing any activity.

When the devices table is overfilled, the application displays the appropriate message.

The devices table contains the following information:

- **Name** – name used to represent a device in the application.
- **Device ID** – device ID assigned in Kaspersky Industrial CyberSecurity for Networks.
- **Status** – asset status that determines whether activity of the device is allowed in the industrial network. A device can have one of the following statuses:
  - *Authorized*. This status is assigned to a device for which activity is allowed in the industrial network.
  - *Unauthorized*. This status is assigned to a device for which activity is not allowed in the industrial network.
  - *Archived*. This status is assigned to a device if it is no longer being used or must not be used in the industrial network, or if the device has shown no activity and the device information has not changed in a long time (30 days or more).
- **Address information** – MAC- and/or IP addresses of the device. If a device has multiple network interfaces, you can specify different MAC- and/or IP addresses for the device on different network interfaces (up to 512 network interfaces can be indicated in the device information). If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the devices table. When you view information about a device, the information about the MAC and / or IP address of the device and address spaces are displayed on the **Addresses** tab.

- **Category** – name of the category that determines the functional purpose of the device. Kaspersky Industrial CyberSecurity for Networks supports the following categories of devices:
    - **PLC** – programmable logic controllers.
    - **IED** – intelligent electronic devices.
    - **HMI / SCADA** – computers with installed software for human-machine interface (HMI) systems or SCADA systems.
    - **Engineering workstation** – computers with installed software to be used by ICS engineers.
    - **Server** – devices with server software installed.
    - **Network device** – network equipment (for example, routers, switches).
    - **Workstation** – desktop personal computers or operator workstations.
    - **Mobile device** – portable electronic devices with computer functionality.
    - **Laptop** – portable PCs.
    - **HMI panel** – devices that use a human-machine interface to manage individual devices or operations of the industrial process.
    - **Printer** – printing devices.
    - **UPS** – uninterruptible power supply units connected to a computer network.
    - **Network camera** – devices that perform video surveillance functions and transmit digital images.
    - **Gateway** – devices that connect networks by converting various interfaces (for example, Serial/Ethernet) within networks that use a different data transfer medium and different protocols.
    - **Storage system** – devices used for storing information in storage systems.
    - **Firewall** – devices that perform firewall functions to inspect and block unwanted traffic.
    - **Switch** – devices used for a physical connection between LAN nodes.
    - **Virtual switch** – devices that logically merge physical switches, or software-implemented switches for virtualization systems.
    - **Router** – devices that redirect network packets between segments of a computer network.
    - **Virtual router** – devices that logically merge physical routers, or routers that utilize multiple independent routing tables.
    - **Wi-Fi** – access points that provide a wireless connection for devices from Wi-Fi networks.
    - **Historian server** – archived data servers.
    - **Other** – devices that do not fall into the categories described above.
- **Group** – name of the group containing the device in the device group tree (contains the name of the group and the names of all its parent groups).

- **Security state** – device security state determined by the presence of events linked to the device. The following security states are available:
  - *Critical*. Events associated with the device have severity rating 8.0–10.0.
  - *Warning*. Events associated with the device have severity rating 4.0–7.9.
  - *OK*. Events associated with the device have severity rating 0.0–3.9, or the device has no associated events.
- **Importance** – importance of the device for the enterprise. Importance is assigned to a device based on its category. The following device importance values are provided:
  - *High*. Assigned to the devices of the following categories: **PLC**, **IED**, **HMI / SCADA**, or **Server**.
  - *Medium*. Assigned to the devices of the following categories: **Engineering workstation**, **Network device**, **Workstation**, **HMI panel**, **Gateway**, **Storage system**, **Firewall**, **Switch**, **Virtual switch**, **Router**, **Virtual router**, **Wi-Fi**, or **Historian server**.
  - *Low*. Assigned to the devices of the following categories: **Mobile device**, **Laptop**, **Printer**, **UPS**, **Network camera**, or **Other**.
- **Last seen** – date and time when the last activity of the device was registered.
- **Risks** – risk categories detected for the device. By default, the device table displays information for current risks only. To display information on all risks, select the **Show remediated and accepted risks** check box when configuring the device table.
- **Last modified** – date and time when information about the device was last modified.
- **Created** – date and time when the device was added to the devices table.
- **OS** – name of the operating system installed on the device.
- **Hardware vendor** – name of the device hardware vendor.
- **Hardware model** – device model name.
- **Hardware version** – device hardware version number.
- **Software vendor** – name of the device software vendor.
- **Software name** – name of the device software.
- **Software version** – device software version number.
- **Network name** – name used to represent the device in the network.
- **Labels** – list of labels assigned to a device.
- **Process Control settings** – indicator of whether there are Process Control settings defined for the device. When you view information about a device, the **Process Control settings** tab displays the Process Control settings configured for the device.
- **EPP application** – concise name of the EPP application installed on the device (if data from this application was received in Kaspersky Industrial CyberSecurity for Networks).

- **EPP connection** – status of the connection between the integration server and the EPP application installed on the device. The following statuses are available:
  - *Active*. Less than 24 hours have passed since the last connection between the application and the integration server.
  - *Inactive*. More than 24 hours have passed since the last connection between the program and the integration server.
  - *N/A*. The status of the connection is unknown.
- **Last connection to EPP** – date of the last connection between the integration server and the EPP application installed on the device.

When viewing the device table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing device information

Detailed information about a device includes information from the device table, and the following fields (if values are available for these fields):

- **Router** – indicator of a routing device.

  > If the router indicator is not determined automatically, it must be set manually, for example, for a device that performs the functions of a network switch between the industrial network segments. This attribute allows the application to use additional algorithms for detecting devices that interact with each other through a router. In particular, if the router indicator is set, either automatically or manually, for a network switch that connects a segment with several PLCs and a computer segment with a SCADA system, the application is able to detect and add to the device table all new devices in the first segment that interact with a computer with the SCADA system in the second segment.

- **Additional information** – additional information about a device specified by an application user (for example, a description of the device deployment location).
- **Custom fields** – set of non-standard device information defined by an application user (for example, categories and classes of device protection). Up to 16 custom fields may be specified for a device.
- **Dynamic fields** – set of expanded device information detected in traffic when the device information detection method is being employed. This field is displayed if expanded information was detected by the application.
- **Kaspersky Endpoint Agent** – information about the Kaspersky Endpoint Agent application installed on the device.
- **Topology settings** – tab containing information about the last active poll of the device, as well as information about the device connections to other nodes.
- **Equipment** – tab containing information about BIOS applications and device processors, information about the amount of free RAM and memory on the device local drives, and information about the USB devices and optical drives used. The information is displayed on the **Equipment** tab if the information is detected by the application.

To view device information:

On the **Devices** tab in the **Assets** section, select the relevant device.

The details area appears in the right part of the web interface window. The details area displays all data that has defined values. Information for which automatic updates are disabled is marked by the 🔒 icon.

Automatically adding and updating devices

The application can automatically add devices to the table and update information about devices. To automatically add and update devices in Kaspersky Industrial CyberSecurity for Networks, you must enable the following asset management methods:

- Device activity detection When using this method, the application adds newly detected devices to the table based on the obtained MAC- and/or IP addresses of the devices. If the application detects activity of an already known device, it may change its status depending on the current asset management mode.
- Device Information Detection When using this method, the application updates information about known devices based on data received from traffic or from EPP applications. Based on data received from traffic, the application updates the information for which automatic updates are enabled in the device settings (this is enabled by default until an application user manually changes a value). If device information detection is disabled, the application does not update or augment available device information based on data received from traffic or from EPP applications.

When adding a device, the application assigns a device name based on the default template: **Device <value of the internal device counter>**. The value of the internal counter in the device name may differ from the device ID that is displayed in the **Device ID** column.

Using device information detection, the application can update a device name after receiving the following information:

- Device model name.
- Network name used to represent the device on the network (the network name of the device takes priority during an update).

The application can automatically update information related to the vendors of network equipment based on the MAC addresses of devices. To identify vendors based on MAC addresses, the application compares the MAC addresses of devices with the address ranges that are registered in the public database of the international Institute of Electrical and Electronics Engineers (IEEE). If a network equipment vendor is identified by MAC address, the application uses the same vendor name that is presented in the IEEE database.

> After the application is installed, it uses a copy of the IEEE database containing information about MAC addresses and vendors that was up to date when the current version of the application was released. You can keep the local copy of the IEEE database up to date by installing updates.

Automatically assigning the statuses of devices

When monitoring the activity of devices in the industrial network, the application can automatically assign statuses to detected devices based on the obtained MAC- and/or IP addresses of devices. Statuses are assigned depending on the current asset management mode.

In learning mode, the application assigns the *Authorized* status to all detected devices (this includes new devices as well as devices that were previously added to the devices table). The status of a detected device is not changed if the *Unauthorized* status was previously assigned to the device.

In monitoring mode, the assigned status depends on whether the device that showed activity is known or unknown to the application. In this mode, statuses are assigned according to the following rules:

- If a device is new (not present in the devices table when it is detected), the *Unauthorized* status is assigned to this device.
- If the device is in the devices table and has the *Authorized* or *Unauthorized* status, the status is not changed.
- If the device is in the devices table with the *Archived* status, the *Unauthorized* status is assigned to this device.

By default, if a device with the *Authorized* status has not shown any activity in over 30 days and the device information has not changed during this time, the *Archived* status is assigned to this device. You can disable automatic device status change to *Archived* when manually changing the status of a device (for example, to prevent the *Authorized* status from automatically changing to the *Archived* status for rarely connected devices).

When devices with the *Unauthorized* status appear in the devices table, you need to determine whether all of these devices are required for industrial process support. After making this determination, it is recommended to manually assign one of the following statuses to each device:

- *Authorized* – if the device is required for industrial process support.
- *Archived* – if the device should not be used in the industrial network.

> Instead of assigning the *Archived* status, you can delete the device. However, all information specified for the device will also be deleted. If a deleted device is detected again, the application will provide only the information that has been received since the device was re-added to the devices table (the date and time of the first detection of the device is also updated).

Device group tree

The device group tree is intended for arranging devices according to their purpose, location, or any other attribute. Devices can be arranged into groups either manually (for example, to designate the location of devices within the facility's industrial structure) or automatically (based on the subnets of device IP addresses, according to the device category, or by vendor).

If a device was not added to any of the groups, this device is assigned to the top level of the group tree hierarchy. By default, devices that are automatically added to the table are not put into groups.

Only users with the Administrator role can put devices into groups.

You can find out which devices belong to groups when viewing the devices table. Paths to groups are indicated in the **Group** column. Device groups are also displayed on the network interactions map. However, devices that are in these groups might not be displayed if they do not satisfy the settings for filtering objects on the network interactions map.

Monitoring read and write of PLC projects

Kaspersky Industrial CyberSecurity for Networks can monitor industrial network traffic for information about PLC projects and compare this information with previously received information about PLC projects.

A PLC project is a microprogram written for a PLC. A PLC project is stored in PLC memory and is run as part of the industrial process that uses the PLC. A PLC project may consist of blocks that are individually transmitted and received over the network when the project is read or written.

Information about a PLC project/block may be received by the application when it detects operations for reading a project/block from a PLC or writing a project/block to a PLC. The obtained information is saved in Kaspersky Industrial CyberSecurity for Networks. The next time it detects a project/block write or read operation, the application compares the received information about the project/block with the saved information. If the received information about a project/block does not match the latest saved information about that project/block (including when there is no saved information), the application registers the corresponding event.

Receiving information about PLC projects is supported for the following types of devices:

- Emerson DeltaV
- Schneider Electric Modicon: M580, M340
- Siemens SIPROTEC 4 and SIMATIC S7-300, S7-400, S7-1200, S7-1500

You do not need to add Process Control settings for devices to monitor read/write of PLC projects. Read/write of PLC projects is monitored for all detected devices of the listed types.

For each device, the application saves no more than 100 different variants of PLC projects. If a PLC project is transmitted or received by individual blocks, up to 100 different variants of each block are saved.

If the maximum number of saved PLC projects (or PLC project blocks with the same name) has been reached for a device, the application saves a newly detected project/block in place of the oldest project/block.

When monitoring read/write of PLC projects, the application registers events based on Asset Management technology. Events are registered with system event types that are assigned the following codes:

- Codes of event types when a PLC project/block is read:
  - 4000005200 – for a detected read of an unknown block of a project from a PLC (if there is no saved information about this block).
  - 4000005201 – for a detected read of a known block of a project from a PLC (if there is saved information about this block but the obtained information does not match the latest saved information about this block).
  - 4000005204 – for a detected read of an unknown project from a PLC (if there is no saved information about this project).
  - 4000005205 – for a detected read of a known project from a PLC (if there is saved information about this project but the obtained information does not match the latest saved information about this project).
- Codes of event types when a project/block is written to a PLC:
  - 4000005202 – for a detected write of a new block of a project to a PLC (if there is no saved information about this block).
  - 4000005203 – for a detected write of a known block of a project to a PLC (if there is saved information about this block but the obtained information does not match the latest saved information about this block).

- 4000005206 – for a detected write of a new project to a PLC (if there is no saved information about this project).
- 4000005207 – for a detected write of a known project to a PLC (if there is saved information about this project but the obtained information does not match the latest saved information about this project).

You can configure the available parameters for event types under **Settings → Event types**.

You can view information about registered events when connected to the Server through the web interface.

Monitoring device equipment

Kaspersky Industrial CyberSecurity for Networks can monitor the equipment of the devices known to the application. While monitoring equipment, the application automatically receives information about the device equipment and registers events when the equipment or its characteristics change.

Equipment monitoring is performed based on the data received from EPP applications. Therefore, to use the equipment monitoring functionality, prepare the application to receive data from EPP applications. For this purpose, the Device Information Detection method must be enabled on the integration server nodes.

The device equipment information is updated once a day. The information for which automatic update is disabled upon adding a device or changing the device information is not updated. The capability to disable automatic update is not available for some equipment details.

The equipment monitoring functionality allows the application to get information listed in the table below.

Information received during equipment monitoring

Information type	Displayed on the tab in the device details area	Ability to disable automatic update
Processors	**Equipment**	—
BIOS	**Equipment**	—
RAM	**Equipment**	—
Local drives	**Equipment**	—
Optical drives	**Equipment**	—
USB devices	**Equipment**	—
Network interfaces with MAC address	**Addresses**	✓
Hardware vendor	**General**	✓
Equipment model	**General**	✓
Equipment version	**General**	✓

When monitoring equipment, the application registers events based on the Asset Management technology. Events are registered with system event types that are assigned the following codes:

- 4000005015 – for an event of adding, changing, or deleting any of the following types of information:
  - Processors
  - BIOS
  - RAM
  - Local drives

  - Optical drives
  - USB devices
- 4000005008 – for the event of receiving new information about the network interface.
- 4000005004 – for the event of receiving new information about the vendor, model, or hardware version.

You can configure the available parameters for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Working with the network interactions map

The network interactions map is a visual representation of detected communications between the devices in the industrial network. You can use the network interactions map to view information about communication between devices during various time periods.

The following objects can be displayed on the network interactions map:

- Nodes. These objects designate the sources and destinations of network packets.
- Device groups. These objects correspond to groups in the device group tree. Groups contain nodes that represent the devices and child groups embedded in those groups.
- Links. These objects represent connections between nodes.

Nodes and links appear on the network interactions map based on data received from traffic or from EPP applications for a specific time interval. Device groups are continually displayed.

If necessary, you can filter nodes and links. By default, the network interactions map displays objects in online mode with a defined filtering period of one hour.

Objects with issues are visually distinguished on the network interactions map. The application considers the following to be objects with issues:

- A node, if there are unprocessed events with a score 4.0 or higher associated with this node, or if this node represents a device with the *Unauthorized* status.
- A connection, if there are events with a score 4.0 or higher associated with this connection. Events registered during the defined object filtering period are taken into account. However, the current status of events is not taken into account.
- Group that contains devices with issues, or whose nodes have links with issues. This includes objects within the group and within any child group of all nesting levels.

Nodes on the network interactions map

Nodes on the network interactions map can be of the following types:

- A device that is known to the application. This type of node represents a device that is listed in the devices table.

- A device that is unknown to the application. This type of node represents a device with a unique IP address or MAC address that is not in the devices table. Such a node may appear on the network interactions map, for example, if network packets are sent using the `ping` command to the address of a non-existent device. Nodes corresponding to unknown devices are displayed individually if their total number does not exceed 100 (according to the current filter settings on the network interactions map). If the number of nodes exceeds this limit, one consolidated node of unknown devices is displayed.

- WAN. This type of node represents devices of a Wide Area Network with which industrial network devices connect. WAN devices are any devices whose IP addresses belong only to **Public** subnets known to the application.

Displayed information on nodes representing devices

The following information is displayed for the nodes corresponding to known devices when the network interactions map is maximized:

- Assigned device name.

- Device category icon.

- IP address of the device (If an IP address is not assigned, the MAC address is displayed).

- Various icons depending on fulfillment of the following conditions:

  - If the router indicator has been set for the device.

  - If an EPP application is installed on the device (the color of the icon depends on the connection state).

  - If the device has the *Archived* status.

- The thick line on the left border of a node has one of the following colors depending on the device's security state:

  - Green signifies the *OK* security state.

  - Yellow signifies the *Warning* security state.

  - Red signifies the *Critical* security state.

If a device has the *Unauthorized* status or has a security state different from the *OK* state, the node has a red background.

Information displayed on nodes representing unknown devices

The following information is displayed for the nodes corresponding to unknown devices when the network interactions map is maximized:

- If a node represents one unknown device, the IP address or MAC address of the device is displayed. For a consolidated node of unknown devices (a node that combines more than 100 unknown devices), **Unknown devices** is displayed.

- Icon for an unknown device and its status ❔ .

Nodes representing devices that are unknown to the application have a gray background.

Displayed information on WAN nodes

The following information is displayed for WAN nodes when the network interactions map is maximized:

- Node name: **WAN**.
- WAN node icon.

Groups of devices on the network interactions map

Groups belonging to the device group tree may be collapsed or expanded on the network interactions map. Collapsed groups are displayed as icons similar to nodes. Expanded groups are displayed as windows containing their embedded nodes and other groups.

Displayed information on collapsed groups

If a group is collapsed, the following information is displayed when the network interactions map is maximized:

- Group name.
- Number of devices that satisfy the current filter settings on the network interactions map. This number includes devices within the group and within its child groups in all nesting levels.
- Number of child groups in all nesting levels.

If a group contains devices or links with issues (including in child groups of any nesting level), the border of this group is colored red.

Displayed information on expanded groups

The window of an expanded group contains a title with the group name and an area for displaying objects. The group window displays the devices included in this group, and the child groups of the next nesting level. Of the devices included in the group, only the devices that meet the current filter settings are displayed on the network interactions map.

If a group contains devices or links with issues (including in child groups of any nesting level), the window has a red background.

Collapsing and expanding groups

If a group is collapsed, you can expand it by double-clicking the icon of the group. If a group is expanded, you can collapse it by double-clicking the header of this group's window or by clicking the ↙ button in the header.

To simultaneously expand multiple collapsed groups:

1. On the network interactions map, select multiple collapsed groups by performing one of the following actions:
   - Hold down the **`SHIFT`** key and use your mouse to select a rectangular area containing the relevant groups.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant collapsed groups.

2. Click ⤢ on the toolbar located in the left part of the network interactions map display area (the button is available if at least one collapsed group is selected).

To simultaneously collapse all expanded groups:

Click ↙ on the toolbar located in the left part of the network interactions map display area (the button is available if at least one group is expanded).

Links on the network interactions map

Links on the network interactions map are identified based on detected network packets for which the source and destination addresses can be mapped to the addresses of nodes.

Each link shows two sides of communication. A communication side in a link may be one of the following objects on the network interactions map:

- One of the following types of nodes:
  - Device that is known to the application.
  - Device that is unknown to the application.
  - Consolidated node of unknown devices – if the link shows communication with one or more unknown devices of this node.
  - WAN node – if the link shows communication in which the source of network packets is a WAN device (the IP address belongs only to **Public** networks that are known to the application).
- Collapsed group, if the link shows communication with one or more devices in this group.

Depending on the scores of the events registered when communications are detected, the link may have the one of following colors:

- Gray – the communication did not cause event registration, or only events with score of 0.0–3.9 were registered.
- Red – the communication caused the registration of events with score of 4.0–10.0.

Events registered during the defined object filtering period are taken into account for links. However, the current status of events is not taken into account.

The application saves connection data in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for the network interactions map when configuring data storage settings on the Server node.

Viewing details about objects

Detailed information about objects on the network interactions map are displayed in the details area. To display detailed information, you can use your mouse to select an object (if you want to view information about a group, you must first collapse the group).

The following information is displayed for nodes:

- If a node represents a known device, the details area displays the same information that is displayed in the devices table.
- If a node represents one unknown device, the details area displays the MAC address and/or IP address of the device (including the names of address spaces if additional address spaces were added to the application).
- If a consolidated node of unknown devices is selected, the following information is displayed:
  - Number of nodes combined by this node under the current filter settings.
  - **IP addresses** – number of IP addresses of unknown devices and the first 100 IP addresses (including the names of address spaces if additional address spaces were added to the application). This section is displayed if there are nodes with IP addresses among the nodes of unknown devices.
  - **MAC addresses** – number of MAC addresses of unknown devices and the first 100 MAC addresses (including the names of address spaces if additional address spaces were added to the application). This section is displayed if there are nodes with MAC addresses among the nodes of unknown devices.
- If a WAN node is selected, the following information is displayed:
  - **Exclude defined addresses** indicates that all devices whose addresses are included in the listed subnets are excluded from the device group.
  - **Subnets** – section containing a list of known subnets indicated as **Public** (external networks).

The following information is displayed for groups:

- **Parent group** – path to the group in the device group tree. If a group belongs to the top hierarchy level, the **N/A (this is a top-level group)** level is displayed.
- Number of devices and groups within the selected group and its child groups of all nesting levels.
- Information about the number of objects with issues within the selected group and its child groups of all nesting levels. If there are no such objects, the *OK* security state is displayed.

The following information is displayed for links:

- **Severity** – icon corresponding to the maximum severity level of events associated with the link. If no event is associated with the link, **No events** is displayed. Events registered during the defined object filtering period are taken into account. However, the current status of events is not taken into account.
- Sections containing basic information about the first and second sides of communication:
  - If the side of communication is a node of a known device or a node of an unknown device, the section displays the name or address of the device/device, category, and address information (for a known device, address information is provided only for those network interfaces that were used during the communication). The device status is also displayed for known devices.
  - If the side of communication is a collapsed group, the section displays the name of the group and the number of devices and child groups within it.
  - If the side of communication is a consolidated node of unknown devices, the section displays the **Unknown devices** node name and the number of nodes combined within this node.
- **Protocols** – section containing a list of protocols used for communication. The volume of transmitted data calculated for detected network packets is specified for each protocol. This section is not displayed if one of the sides of communication is a consolidated node of unknown devices.

Changing the scale of the network interactions map

The network interactions map can be displayed in a scale of 1–100%. The current scale is displayed on the toolbar located in the left part of the network interactions map display area.

To change the scale of the network interactions map:

Use the mouse wheel or the **+** and **–** buttons located in the toolbar next to the current scale value.

Reducing the scale of the network interactions map reduces the amount of information that is displayed for the nodes and collapsed groups.

If the display scale is less than 25%, icons and text information are not displayed in nodes and collapsed groups. The appearance of nodes and collapsed groups may change as follows:

- On a node representing a device that is known to the application (device), the upper-right corner displays the device status as a triangle in one of the following colors:
  - Green signifies that the device has the *Authorized* status.
  - Red signifies that the device has the *Unauthorized* status.
  - Gray signifies that the device has the *Archived* status.
- A thick black line on the left border of the node appears on the WAN node.
- On a collapsed group, the upper-right corner displays a triangle indicating the presence of objects with issues. The triangle has one of the following colors:
  - Green means that the group does not contain objects with issues.
  - Red means that the group contains objects with issues.

Positioning the network interactions map

If necessary, you can change the positioning of the network interactions map manually or automatically. Automatic positioning lets you move the network interactions map and change its scale to display all nodes that satisfy the defined filter settings, as well as all expanded groups.

To manually position the network interactions map:

1. Position the mouse pointer over any part of the network interactions map that is not occupied by objects.
2. Click and hold the left mouse button to drag the network interactions map.

To automatically position the network interactions map:

Click the ⤢ button on the toolbar located in the left part of the network interactions map display area.

The positioning and the scale of the network interactions map will change to display all nodes and expanded groups.

Pinning and unpinning nodes and groups

By default, nodes and collapsed groups are not pinned on the network interactions map. Unpinned nodes and collapsed groups may be automatically arranged for optimal display of other objects.

Nodes and groups are pinned when their location is changed manually or when automatically arranged. You can also pin the current location of displayed objects without moving them.

To pin and unpin objects without moving them, you can use the following interface elements:

- The buttons on the toolbar located in the left part of the network interactions map display area. You can use the 📌 and ⚲ buttons to pin and unpin all nodes and groups displayed on the network interactions map (including nodes in expanded groups).
- Buttons in the expanded group's window header. You can use the 📌 and ⚲ buttons to pin and unpin only nodes and groups in the window of the expanded group (but not in windows of nested groups).

The buttons are available if the network interactions map contains the objects to which the corresponding actions can be applied.

After the location of a node or collapsed group is pinned, the 📌 icon appears in the upper-right corner of this element (if the scale of the network interactions map is not less than 25%). You can also use this icon to unpin the object.

The location of a pinned node or pinned group is retained. If a pinned node disappears from the network interactions map (for example, as a result of filtering), this node will be displayed in the same location the next time it appears.

Manually changing the location of nodes and groups

You can manually change location of nodes and groups on the network interactions map by arranging them in the most convenient way for you.

After their arrangement, nodes and groups are locked (pinned) in their new location. If necessary, you can unpin these objects.

Objects that are included in groups can be moved only within the windows of these groups.

To change the location of nodes and/or collapsed groups:

1. On the network interactions map, select one or multiple objects corresponding to nodes and/or collapsed groups.

   To select multiple nodes and/or collapsed groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.
2. Use your mouse to drag the selected objects to the necessary location.

After they are moved, nodes and collapsed groups will remain pinned. The 📌 icon appears in these objects.

To change the location of an expanded group:

Move the cursor over the expanded group's window title, left-click and drag the window to the necessary location.

Automatic arrangement of nodes and groups

For optimal arrangement of objects on the network interactions map, you can use algorithms to automatically change the location (arrangement) of nodes and groups. The following algorithms are provided:

- Radial arrangement.
- Grid-aligned arrangement.

You can use automatic arrangement algorithms for the following objects:

- All displayed nodes and groups at the top level of the hierarchy within the group tree. Automatic arrangement is performed using the ☰ (radial arrangement) button and the ⠿ (grid-aligned arrangement) button on the toolbar located in the left part of the network interactions map display area.
- All displayed nodes and groups within the expanded group. Automatic arrangement is performed by using the ☰ (radial arrangement) button and ⠿ (grid-aligned arrangement) button in the expanded group's window header.
- Only selected nodes and collapsed groups. Before performing automatic arrangement, you need to select at least three nodes and/or collapsed groups within the expanded group or at the top level of the hierarchy. To select multiple objects, you can use the mouse to select a rectangular area containing the relevant objects while holding down the **`SHIFT`** key, or select the relevant objects with the mouse while holding down the **`CTRL`** key. Automatic arrangement is performed using the ☰ (radial arrangement) button and the ⠿ (grid-aligned arrangement) button on the toolbar located in the left part of the network interactions map display area.

After automatic arrangement, nodes and groups are locked (pinned) in their new location. The 📌 icon appears in these objects. If necessary, you can unpin these objects.

Searching for nodes on the network map

You can search nodes on the network interactions map based on information about these nodes. This search involves all nodes that meet the current filter settings, including those located in collapsed groups or outside of the displayed part of the network interactions map.

For nodes representing known devices, the search is performed in all columns of the devices table except the following columns: **Status**, **Security state**, **Last seen**, **Last modified**, and **Created**. The search is also performed in the values of custom fields for devices.

To find the nodes on the network interactions map:

In the **Network map** section, enter your search query into the **Search nodes** field. The search is initiated as you type characters in the search field.

If nodes that satisfy the search query are found, the contours of these nodes are highlighted in yellow. The contours of collapsed groups in which nodes were found are highlighted in the same way. However, the right part of the **Search nodes** field will display the following items:

- Sequence number of the currently selected object (node or collapsed group containing the found nodes) among the search results.
- Total number of found objects (nodes and/or collapsed groups containing the found nodes).

  > The number of nodes in collapsed groups is not taken into account in the total number of found objects. If you want the nodes in groups to also be taken into account in the search results, expand the collapsed groups.

- Arrows for moving between found objects. Arrow movements proceed in alphabetical order of the names of found objects. When moving to the next object, the network interactions map is automatically positioned to display this object.

Filtering objects on the network interactions map

To limit the number of nodes and links displayed on the network interactions map, use the following functions:

- Functions for complex filtering of nodes and links:
  - Filtering using a period on the time scale ?

To filter nodes and links, you can choose the relevant period of time on the time scale. The time scale is displayed in the lower part of the **Network interactions map** tab of the **Network map** section.

The time scale contains the following items:

- Time scale start date and time.
- Periods when events with scores of 4.0 and above were registered. These periods are displayed as red strips in the lower part of the time scale. The periods are not displayed if a duration of more than seven days is defined for the time scale.
- Filtering period. This period is displayed as a yellow band lined with buttons for moving the boundaries.
- Chart of the volume of traffic processed by the application. The chart is not displayed if a duration of more than seven days is defined for the time scale.
- End of the time scale. Depending on the arrangement of the filtering period, the end of the time scale is displayed as a date and time (if the date and time are defined) or as a **Now** link.

The following types of filtering periods are provided:

- Period correlated to the current moment. The right-side boundary of this period corresponds to the time scale boundary designating the current moment in time.
- Period not correlated to the current moment. This type of period may be arranged in any part of the time scale.

To configure object filtering by a period correlated to the current moment:

1. Click the **Now** button on the right of the time scale. This button is not displayed if the period is already correlated to the current moment.
2. If it is necessary to specify a different period duration, perform one of the following actions:
   - Move the left border of the yellow band of the period to the necessary position (the maximum duration of the period is 7 days).
   - Open the configuration window by using the button above the yellow band of the period, select the **Anchor to boundary** check box, select the necessary duration (**Hour**, **Day**, **7 days**), and click **OK**.

   The network interactions map shows only the nodes and links for which communications were detected since the beginning of the specified period up to the current moment.

To configure filtering by a period not correlated to the current moment:

1. If the necessary period is not within the time scale, change the values of the date and time for the start and/or end of the time scale:
   a. To change the data and time of the start of the time scale, open the window by clicking the link in the left part of the time scale and select one of the following options:
      - **Day**
      - **7 days**

    - **30 days**
    - **Specify a date**. For this option, specify a date and time in the opened field

   b. To change the date and time of the end of the time scale, open the window by clicking the link in the right part of the time scale and select one of the following options:

    - **Now**
    - **Specify a date**. For this option, specify a date and time in the opened field

2. Specify the necessary period. To do so, do one of the following:

   - Use the mouse to move the period to the relevant place on the time scale.
   - Move one or both of the borders of the yellow band of the period to the necessary part of the time scale (the maximum duration of the period is 7 days).
   - Open the configuration window by using the button above the yellow band of the period, select the necessary duration (**Hour**, **Day**, **7 days**), and click **OK**.

3. If a period is automatically anchored to the current moment (when you move the period to the right-most position, the **Now** button on the right of the time scale is no longer displayed), disable automatic anchoring of the period to the time scale boundary. To do so, open the configuration window by using the button above the yellow band of the period, clear the **Anchor to boundary** check box, and click **OK**.

- Filtering by registered events ?

You can configure the network interactions map to show the nodes and links whose information is saved in the events associated with the selected nodes.

The capability to filter by events is available if no more than 200 nodes are selected on the network interactions map. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

You can use the following methods to filter by event:

- Initial filtering by event. This method is applied if you need to filter objects based on events associated only with the selected nodes.
- Additional filtering by event. This method is applied if initial filtering by events is already performed (for example, when switching to the network interactions map from the events table) and you need also to filter events associated with additionally selected nodes from the list of nodes displayed on the network interactions map.

To display nodes and links using initial filtering by event:

1. On the network interactions map, select one or multiple objects corresponding to nodes and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the `SHIFT` key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the `CTRL` key and use your mouse to select the relevant objects.
2. On the toolbar located above the network interactions map, open the **Event filter** drop-down list.
3. In the drop-down list, select **Filter**.

The network interactions map displays only the nodes and links whose information is contained in the events associated with the selected nodes. The toolbar located above the network interactions map displays a list containing the IDs of events (IDs are listed in the order in which their associated events were detected).

To add nodes and links to the displayed objects by using additional filtering by event:

1. Make sure that initial filtering by event has been performed. To do so, check for the availability of a list containing event IDs on the toolbar located above the network interactions map.
2. Among the nodes displayed on the network interactions map, select the nodes for which you want to add associated events to the filter.

   The details area appears in the right part of the web interface window.
3. On the toolbar located above the network interactions map, open the **Event filter** drop-down list.
4. In the drop-down list, select **Add to filter**.

The network interactions map also displays the nodes and links whose information is contained in the events associated with the selected nodes. The IDs of detected events are added to the list containing IDs in the toolbar.

- Functions for filtering nodes:
  - Filtering by device status
    1. On the toolbar located above the network interactions map, open the **Device statuses** drop-down list.

       You will see a list containing the names of statuses for devices that are known to the application (**Unauthorized**, **Authorized**, **Archived**), and the **Unknown device** status for devices that are unknown to the application.
    2. In the drop-down list, select the check boxes for the statuses of devices that need to be displayed on the network interactions map.
    3. Click **OK**.

    The network interactions map displays only the nodes corresponding to devices with the selected statuses.
  - Filtering by device security state
    1. On the toolbar located above the network interactions map, open the **Device states** drop-down list.

       You will see a list containing the names of security states for devices (**OK**, **Warning**, **Critical**).
    2. In the drop-down list, select the check boxes for the security states of nodes that need to be displayed on the network interactions map.
    3. Click **OK**.

    The network interactions map displays only the nodes corresponding to devices with the selected security states.
  - Filtering by device category
    1. On the toolbar located above the network interactions map, open the **Device categories** drop-down list.

       You will see a list containing the names of categories for known devices, as well as individual categories for unknown devices and WAN nodes.
    2. In the drop-down list, select the check boxes for the categories of devices that need to be displayed on the network interactions map.
    3. Click **OK**.

    The network interactions map displays only the nodes corresponding to devices with the selected categories.
  - Enabling and disabling the display of nodes associated with filtered nodes

After filtering nodes, the network interactions map displays only the nodes that satisfy the defined filter settings. In addition, for a node to be displayed on the network interactions map, it must have a connection (link) with another displayed node. If, according to the specified filtering parameters, the network interactions map does not display any node with which a node has interacted, this node is also not displayed on the network interactions map. Filtering is applied similarly for nodes that are part of a consolidated node of unknown devices: if the network map does not display all nodes with which a node of an unknown device has interacted, this node is removed from the list of nodes within the consolidated node of unknown devices.

If necessary, you can enable the network interactions map to display all nodes associated with filtered nodes. Together with the nodes that satisfy the defined node filtering criteria, the network interactions map also displays all nodes with which these nodes have interactions (irrespective of the defined filter settings).

For example, if the nodes are filtered by the **PLC** category and you enabled the display of linked nodes, the network interactions map will display all nodes that have communicated with **PLC** category devices. If the display of linked nodes is disabled, the network interactions map will display nodes corresponding only to those **PLC** category devices that have communicated with each other.

To enable or disable the display of nodes associated with filtered nodes:

Use the **Linked devices** toggle button on the toolbar located above the network interactions map.

- Functions for filtering links:
  - Filtering by link severity scores ?

1. On the toolbar located above the network interactions map, open the **Scores of links** drop-down list.

   A list is displayed that contains the names of event severity levels with their score ranges (**Low (0.0 - 3.9)**, **Medium (4.0 - 7.9)**, **High (8.0 - 10.0)**), as well as the **No events** element, which allows you to filter the connections for which no events are registered.

2. In the drop-down list, select the check boxes for those severity levels by which you want to filter links.

3. Click **OK**.

The network interactions map displays only the links associated with events that have the selected severity levels.

  - Filtering by communication protocols ?

1. On the toolbar located above the network interactions map, open the **Protocol** drop-down list.

   You will see a window containing the table of supported protocols displayed as a protocol stack tree. You can manage how tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   The table columns provide the following information:

   - **Protocol** – name of the protocol within the protocol stack tree.
   - **EtherType** – number of the next-level protocol within the Ethernet protocol (if the protocol has a defined number). It is displayed in decimal format.
   - **IP number** – number of the next-level protocol within the IP protocol (if the protocol has a defined number). It is indicated only for protocols within the IP protocol structure. It is displayed in decimal format.

2. If necessary, use the search field above the table to find relevant protocols.
3. In the list of protocols, select the check boxes opposite the protocols by which you want to filter events.

   If you select or clear the check box for a protocol that contains nested protocols, the check boxes for the nested protocols are also automatically selected or cleared.

4. Click **OK**.

The network interactions map displays only the links for which the selected protocols are used.

- Filtering based on the OSI model layers ?

You can filter links based on the levels of communications corresponding to the layers of the OSI (Open Systems Interconnection) model for the network protocol stack.

To filter links on the network interactions map based on the layers of the OSI network model:

1. On the toolbar located above the network interactions map, open the **OSI model layers** drop-down list.

   You will see a list containing the names of OSI model layers:

   - **Data Link**. This layer includes the communication links in which MAC addresses were used to communicate with devices.
   - **Network**. This layer includes links in which IP addresses were used to communicate with devices.

2. In the drop-down list, select the check boxes for the OSI model layers whose links need to be displayed on the network interactions map.
3. Click **OK**.

The interaction network map displays only the links that are associated with the selected OSI model layer.

- Resetting the filter settings ?

You can reset the defined settings for filtering nodes and links to their default state.

To reset the defined filter settings on the network interactions map:

On the toolbar located above the network interactions map, click the **Default filter** button (this button is displayed if filter settings are defined).

The network interactions map will display all nodes and links for which communications within the specified period were detected.

Saving and loading network interactions map display settings

The application lets you save the current network interactions map display settings. A set of saved display settings is called a *view*. You can use views to apply the saved display settings of the network interactions map (for example, to quickly restore the display settings after making some changes, or to work with the network interactions map on a different computer).

When a network interactions map view is saved, the following display settings are saved:

- Scale
- Network interactions map positioning
- Location of pinned nodes and groups
- Filtering of nodes and links

The application can save and use no more than 10 groups of settings for the different network interactions map views.

Only the users with the Administrator role can manage the list of network interactions map views (including saving the current display settings). However, users with the Administrator role and users with the Operator role can both access the list of views and apply the saved groups of settings.

When working with network interactions map views, you can use the following functions:

- **Adding a new view while saving the current network interactions map display settings**

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, configure the networking map display settings.
3. Open the **Configure network map views** window by clicking the **Manage views** button.
4. Click **Add**.
5. Type the view name in the entry field.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A view name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 100 characters or less.
   - Must not match the name of a different view (not case-sensitive).
6. Click the ✓ icon on the right of the entry field.

- Updating a view while saving the current network interactions map display settings

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Topology map** tab in the **Network map** section, configure the networking map display settings.
3. Open the **Configure network map views** window by clicking the **Manage views** button.
4. Select the view in which you want to save the current network interactions map display settings.
5. Click the **Overwrite** button.

   A window with a confirmation prompt opens.
6. In the prompt window, confirm that you want to save the current settings in the selected view.

- Renaming a network interactions map view

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
3. Select the view that you want to rename.
4. Click the ✎ icon on the right of the current view name.
5. In the entry field, enter the new name of the view.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A view name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 100 characters or less.
   - Must not match the name of a different view (not case-sensitive).
6. Click the ✓ icon on the right of the entry field.

- Deleting a network interactions map view

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
3. Select the view that you want to delete.
4. Click the **Delete** button.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the selected view.

- Applying saved view settings on the network interactions map

1. On the **Network interactions map** tab in the **Network map** section, open the **Configure network map views** window by clicking the **Manage views** button.
2. Select the relevant view in the list.
3. Click the **Apply** button.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm application of the view.

Downloading traffic when working with the network interaction map

When working with the network interactions map, you can download traffic received by the application via the monitoring points. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads traffic from the traffic dump file storages. Both the internal storage of each node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

When downloading traffic, take the following considerations into account:

- Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.
- Only the users with the Administrator role can download traffic when working with the network interactions map.

To download traffic when working with the network interactions map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network interactions map** tab in the **Network map** section, click the **Download traffic** button.

   The details area appears in the right part of the web interface window.
3. Perform the following actions:
   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

     By default, the period is set to the period configured for filtering specified on the time scale.
   - Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

     If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.
   - If necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points that received the desired traffic.

     By default, all monitoring points available on nodes with the installed application components are specified.
   - If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets belong (this section is displayed if additional address spaces are added to the application).

     By default, all address spaces created in the application are specified.
   - If necessary, enable filtering in the **BPF filtering** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

     Filtering expression example:

     ```
     tcp port 102 or tcp port 502
     ```

- If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets.

  Filtering expression example:

  ```
  ^ test. + xABxCD
  ```

4. Click the **Show** button.

5. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Network session monitoring

Kaspersky Industrial CyberSecurity for Networks can detect network sessions created by the devices for connecting with other devices in the industrial network traffic. The application registers the detected network sessions and saves information you can use to analyze the network activity of the devices and download data about transmitted network packets from the traffic dump files. Unlike connections on the network interaction map, registered network sessions provide more detailed information about the device interactions, including because of separate registration of sessions for different ports and protocols that were used in the interactions.

The application detects network sessions if the use of the Network Session Detection method based on the Asset Control technology is enabled. Network session detection can be performed when analyzing traffic received by monitoring points, as well as when receiving data from EPP applications.

Each registered network session contains information about the connection between two devices that are interaction sides. A network session is characterized by the address information of the interaction sides (MAC and / or IP addresses), port numbers, and the application protocol that was used for the connection. The first device in a network session is usually the device that initiates the sending of network packets to the other device.

A network session is considered completed if no network packets are sent during one minute within this session or if the network session detection technology is disabled on the corresponding node or monitoring point.

If an excessive number of network sessions are detected, the application applies the following session registration restrictions:

- The number of registered sessions between the two interaction sides using the same application protocol doesn't exceed 1000 per minute

- The total number of registered sessions between the two interaction sides is no more than 5000 per minute

The application saves network session data in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for the network sessions when configuring data storage settings on the Server node in the **Network sessions** section.

You can view information about network sessions on the **Network sessions** tab in the **Network map** section.

Network sessions table

The network sessions table is displayed on the **Network sessions** tab in the **Network map** section.

The network sessions table contains the following information:

- **Status** – the network session status. A registered network session can have one of the following statuses:
  - *Active*. This status is assigned when a network session is registered and is retained as long as devices within this session send network packets.
  - *Completed*. This status is assigned to a network session if no network packets are sent during one minute within this session or if the network session detection technology is disabled on the corresponding node or monitoring point.
- **Side 1** – MAC and / or IP addresses of the first network interaction side. MAC and IP addresses can be enabled and disabled.
- **Side 1 port** – port number of the first side of the interaction.
- **Side 2** – MAC and / or IP addresses of the second network interaction side. MAC and IP addresses can be enabled and disabled.
- **Side 2 port** – port number of the second side of the interaction.
- **Device 1** – name of a device known to the application to which the address information of the first interaction side corresponds.
- **Device 2** – name of a device known to the application to which the address information of the second interaction side corresponds.
- **Transfer protocol** – transport protocol used in the network session.
- **Application protocol** – application layer protocol used in the network session.
- **Current speed** – current data transfer rate in the network session.
- **Average speed** – average data transfer rate in the network session.
- **Total transmitted** – the number of bytes transmitted in the network session.
- **Monitoring points** – names of the monitoring points that receive the network session traffic.
- **Start** – date and time of the first network packet in the network session or the start date and time of the time interval which data is received from the EPP application.
- **Last interaction** – date and time of the last network packet in the network session or the expiration date and time of the time interval which data is received from the EPP application (if only one packet is received in the network session, the value is the same as the **Start** parameter value).
- **Number of packets** – the number of network packets transmitted in the network session.

When viewing the network session table, you can use configuration, filter, search, and sort functions, navigate to the related items, and export data.

Viewing network session details

Detailed information about the network session includes information from the network sessions table as well as the name of the application during which operation the network session was initiated (if the application was able to determine the name of the application).

To view information about a network session:

On the **Network sessions** tab in the **Network map** section, select the required network session.

The details area appears in the right part of the web interface window. The details area displays all received information about the network session.

Downloading network session traffic

When viewing the network sessions table, you can download the traffic related to the selected network sessions. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads the network session traffic from the traffic dump file storages. Both the internal storage of a node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

When downloading the network session traffic, take the following considerations into account:

- Traffic download is possible only for the network sessions registered during the analysis of traffic received at the monitoring points. If a network session was registered based on the data received from the EPP application, the application cannot download the traffic of this session.
- Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The network session traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.
- Only the users with the Administrator role can download network session traffic.

To download network session traffic:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. On the **Network sessions** tab in the **Network map** section, select the network sessions for which you want to download traffic.

   You can select no more than 100 network sessions.
3. Click the **Download traffic** button.

   The details area appears in the right part of the web interface window.
4. Perform the following actions:
   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

By default, the maximum possible period is specified, from the start date and time of the earliest network session to the end date and time of the latest session from the selected sessions. If necessary, you can set boundaries within this period or set an empty value for one of the boundaries (for example, for the right boundary to download new traffic of the sessions that are not yet completed).

- Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

  If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.

- If necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points that received the desired traffic.

  By default, the monitoring points that receive the traffic of the selected network sessions are specified.

- If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets of the selected network sessions belong (this section is displayed if additional address spaces are added to the application).

  By default, all address spaces created in the application are specified.

- If necessary, enable filtering in the **BPF filtering** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets of the selected network session.

  Filtering expression example:

  ```
  tcp port 102 or tcp port 502
  ```

- If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets of the selected network sessions.

  Filtering expression example:

  ```
  ^ test. + xABxCD
  ```

5. Click the **Show** button.

6. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Monitoring events and incidents

When analyzing industrial network traffic, the application registers events and incidents.

An *event* in Kaspersky Industrial CyberSecurity for Networks is a record containing information about the detection of certain changes or conditions in industrial network traffic requiring the attention of an ICS security officer. Events are registered and transmitted to the Kaspersky Industrial CyberSecurity for Networks Server. The Server processes received events and saves them in a database.

An *incident* is a special type of event that is registered when a certain sequence of events is received. Incidents group events that have certain common traits or that are associated with the same process.

The application registers incidents based on event correlation rules. An *event correlation rule* describes the conditions for checking the sequences of events. When the application detects a sequence of events matching the rule conditions, it registers an incident that indicates the name of the triggered rule. Incidents are registered using the system event type that is assigned the code 8000000001.

Event correlation rules are embedded in the application and are applied regardless of the security policy.

After installation, the application uses the default event correlation rules. To improve the effectiveness of rules, Kaspersky experts regularly update the databases containing the sets of rules. You can update correlation rules by installing updates.

The Kaspersky Industrial CyberSecurity for Networks Server registers events and incidents according to the settings defined for registering event types. You can configure these settings in the Event types section (for all event types) and when configuring Process Control rules (only for events that are registered when Process Control rules are triggered).

To reduce the number of frequently recurring events that do not require attention from the operator, you can create allow rules for events. Events that satisfy allow rules are not registered. For example, you can use an allow rule to temporarily disable registration of all events from a specific monitoring point. You can view allow rules for events in the **Allow rules** section. The EVT type is indicated for these rules.

The application saves events and incidents in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. If the minimum storage time limit is enabled and the application deletes entries whose storage time is less than the defined limit, a corresponding message will appear in the application message log. You can configure the settings for storing events and incidents.

Database files are saved on the Server in the DBMS folders. Deleting or modifying any file in these folders may cause a disruption in application performance.

You can view information about events and incidents in the following sections of the Kaspersky Industrial CyberSecurity for Networks web interface:

- The **Dashboard** section displays general information about the latest events and incidents registered by the application.
- The **Events and incidents** tab of the **Events** section displays detailed information about events and incidents and provides the capability to download information from the Server database for any period.

Scores and severities of events

Events and incidents in Kaspersky Industrial CyberSecurity for Networks are scored on a scale from 0.0 to 10.0.

If an event is linked to a device, the application calculates a numerical value for the score based on available information about the device. When calculating a score in this case, the application considers the level of importance of the device and the risks associated with this device.

The starting value used for calculating the score is the *base score* defined for the specific type of event in the event types table or defined when configuring Process Control rules (only for events that are registered when Process Control rules are triggered).

If an event is not linked to a device, the score of this event is equal to the base score.

This score determines the severity of the event. Depending on the numerical value of its score, an event can have one of the following severities:

- *Low* (scores 0.0–3.9).

  Low-severity events normally do not require an immediate response.

- *Medium* (scores 4.0–7.9).

  Medium-severity events contain information that requires attention. These events may require a response.

- *High* (scores 8.0–10.0).

  High-severity events contain information that may have a critical impact on the industrial process. These events require an immediate response.

To ensure compatibility with the *severity levels* of events that were used in previous versions of the application, the current version of Kaspersky Industrial CyberSecurity for Networks converts those severity levels into the following scores:

- Events with *Informational* severity are assigned a score of 3.0.
- Events with *Warning* severity are assigned a score of 6.0.
- Events with *Critical* severity are assigned a score of 9.0.

Event registration technologies

Kaspersky Industrial CyberSecurity for Networks registers events based on one of the following technologies:

- *Deep Packet Inspection* (DPI)

  This technology is used to register events associated with process violations (for example, an event where the specified temperature was exceeded).

- *Network Integrity Control* (NIC)

  This technology is used to register events associated with industrial network integrity or the security of communications (for example, an event for the detection of communications between devices in the industrial network over a protocol that is new for those devices).

- *Intrusion Detection* (IDS)

  This technology is used to register events associated with the detection of traffic anomalies that are signs of an attack (for example, an event for the detection of signs of ARP spoofing).

- *Command Control* (CC)

  This technology is used to register events associated with the detection of system commands for devices in traffic (for example, an event for the detection of an unauthorized system command).

- *External* (EXT)

This technology is used for incidents and events that are received by Kaspersky Industrial CyberSecurity for Networks from recipient systems using Kaspersky Industrial CyberSecurity for Networks API methods.

- *Asset Management* (AM)

  This technology is used to register events associated with the detection of device information in traffic or in data received from EPP applications (for example, an event for the detection of a new IP address for a device).

- *Endpoint Protection Platform* (EPP)

  This technology is used to register events associated with threats detected by Kaspersky applications that perform functions to protect workstations and servers (for example, a malware detection event).

Event statuses

Statuses of events and incidents enable the application to show the progression of information processing by the ICS security officer.

The following statuses can be assigned to events and incidents:

- *New*

  This status is assigned to all events and incidents when they are registered in Kaspersky Industrial CyberSecurity for Networks.

- *In progress*

  You can assign this status to events and incidents that are currently being processed (in progress), for example, when investigating the reasons for registration of these events and incidents.

- *Resolved*

  You can assign this status to events and incidents that have already been processed (for example, investigation of the reasons for their registration is complete).

  > After the *Resolved* status is assigned, events and incidents with this status are not taken into account by the application when determining the security states of devices displayed in the devices table and on the network interactions map.

The statuses of events and incidents are changed manually. You can sequentially assign statuses in order from the *New* status to the *Resolved* status (however, you are not required to assign the intermediate *In progress* status). After the status of an event or incident is changed, you cannot assign the previous status to it.

Table of registered events

You can view the table of registered events and incidents on the **Events and incidents** tab in the **Events** section.

By default, the table of registered events and incidents is updated in online mode. The beginning of the table displays the events and incidents with the latest dates and times when last visible.

The date and time when the event or incident was last visible may differ from the date and time of its registration (the date and time of registration is displayed in the **Start** column). For an event, the date and time when last visible may be updated during the event regeneration period for this type of event. For an incident, the date and time when last visible is updated according to the date and time of last occurrence of the events that are part of the incident.

The settings of events and incidents are displayed in the following columns of the table:

- **Start**

  For an event that is not an incident – date and time of event registration. For an incident – date and time of registration of the first event included in the incident. In the table, you can view the date together with the time, or just the date or time by itself. To choose the information to display, select the check boxes opposite the **Date** and/or **Time** settings.

- **Last seen**

  For an event that is not an incident, this is the date and time when the event last occurred. It may contain the date and time of event registration, or the date and time when the event regenerate counter value increased if the conditions for event registration were repeated during the event regenerate timeout. The value of the regenerate counter is displayed in the **Total appearances** column. For an incident, this is the latest date and time of last occurrence of events that are part of the incident. Just like with the **Start** column, you can view the date together with the time, or just the date or time by itself.

- **Title**

  Header defined for the event type.

- **Score**

  Calculated value for the event score. The severity of the event is designated by a numerical score. Depending on the severity, the score may have one of the following colors:

  - Red designates an event with *High* severity.
  - Yellow designates an event with *Medium* severity.
  - Blue designates an event with *Low* severity.

- **Source**

  Address of the source of network packets. You can enable or disable the display of addresses and ports of address information by using the following settings (their abbreviated names displayed in table columns are indicated in the parentheses): **IP address**, **Port number (P)**, **MAC address**, **VLAN ID (VID)**, **Application-level address**. If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the devices table.

- **Destination**

  Address of the destination of network packets. The display of address information can be configured the same way as the **Source** column.

- **Protocol**

  Application layer protocol that was being monitored when the application registered the event.

- **Technology**

  This icon corresponds to the technology that was used to register the event.

- **Total appearances**

For an event that is not an incident, this is the value of the regenerate counter after the event is registered within the event regenerate timeout. A value greater than 1 means that the conditions for event registration were repeated N – 1 times. The value 1 is displayed for the incident in this column.

- **ID**

  Unique ID of the registered event or incident.

- **Application**

  Information about applications that were running when event registration conditions occurred. An event saves the application data received from EPP applications.

- **Application user**

  Information about the user account that was used to start the application specified in the **Application** column.

- **Status**

  This icon corresponds to the status of an event or incident.

- **Description**

  Description specified for the event type.

- **End**

  For an event that is not an incident, this is the date and time when the *Resolved* status was assigned, or the date and time of the event regenerate timeout. For an incident, this is the latest date and time of the end of events that are part of the incident. Just like with the **Start** column, you can view the date together with the time, or just the date or time by itself.

- **Triggered rule**

  For an event that is not an incident, this is the name of the Process Control rule or Intrusion Detection rule whose triggering caused the registration of the event. For an incident, this is the name of the correlation rule whose triggering caused the registration of the incident.

- **Monitoring point**

  Monitoring point whose traffic invoked registration of the event.

- **Event type**

  Numerical code assigned to the event type.

- **Marker**

  This is a selection of icons that you can set for any event or incident so that you can easily find events and incidents based on a criterion that is not in the table.

When viewing the table of events and incidents, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing events included in an incident

For viewing events included in incidents, the following modes are provided in the events table:

- Simple viewing mode. In this mode, the events table displays all events without consideration of how events are nested in incidents.

- Tree display mode. In this mode, incidents are displayed as tree structures that can be collapsed or expanded using the ⊞ and ⊟ buttons next to the headers of incidents.

You can change the display mode when configuring the events table.

Viewing event details

Detailed information about events and incidents is displayed in the details area in the **Events** section of the application web interface.

To view the details of an event or incident:

On the **Events and incidents** tab in the **Events** section, select the relevant event or incident.

The right part of the web interface window will show the details area, which displays detailed information about the selected event or incident.

Changing the statuses of events

You can change the following statuses of events and incidents:

- *New* This status can be changed to the *In progress* or *Resolved* status.
- *In progress* This status can be changed to the *Resolved* status.

The *Resolved* status cannot be changed.

If an event is associated with a risk, this event can be assigned the *Resolved* status at the same time as the risk status is changed to the *Accepted* status.

To change the status of events or incidents when working with the events table:

1. Select the **Events and incidents** tab in the **Events** section.
2. In the events table, select the events and/or incidents whose status you want to change.
3. Open the **Change status** drop-down list in the toolbar.
4. In the drop-down list, select the command to assign the required status.

   Some drop-down list items are not available in the following cases:

   - The **In progress** item is unavailable if the selected items do not include events or incidents with the *New* status.
   - The **Resolved** item is unavailable if the selected items do not include events or incidents with the *New* or *In progress* status.

   > If all events and incidents that satisfy the current filter and search settings are selected, and the number of selected items is more than 1,000, the application does not check their statuses. In this case, the **In progress** and **Resolved** items are both available. However, the **In progress** item can be used to assign the *In progress* status only to events and incidents that have the *New* status.

A window with a confirmation prompt opens.

5. If the selected events are associated with risks and you want to simultaneously assign the *Accepted* status to these risks, select the **Set the Accepted status for all risks related to the event** check box (if one event is selected) or the **Set the Accepted status for all risks related to the events** check box (if multiple events are selected).

   Risks may be associated with events when the application registers events of certain types based on Asset Management technology.

6. In the prompt window, click **OK**.

Viewing details of EDR incidents

EPP events may contain information on the threat development chains received from Kaspersky Endpoint Agent. If a threat development chain is built for an event, Kaspersky Industrial CyberSecurity for Networks considers such event an *Endpoint Detection and Response* incident (EDR incident).

A threat development chain is a sequence of activity events on a device associated with a detected threat. A key activity event in the threat development chain is an activity event with a threat detection object. All other activity events in the chain (preceding and following the key activity event) are saved for further threat development analysis.

> Information on the threat development chain built may not be added to the event simultaneously with the registration of this event. The maximum delay in adding this information to an event by the application is 10 hours after its registration. The information is not added if the event has the *Resolved* status.

EDR incidents are marked with the **EDR** icon in the event table. For each EDR incident, you can view information on the threat development chain in the details area. The information is displayed on the following tabs in the details area:

- **Activity event graph** provides visual information about objects involved in the threat development chain. Activity events are represented as nodes on the graph. The nodes are located at different levels in accordance with the identified threat development process. The key activity event is located at the lowest level of the graph. This level can also display nodes that group other activity events by their types. Above this level, the application can display up to four levels with activity event nodes.
- **All activity events** displays table view of the information about all activity events included in the threat development chain and presented as nodes in the activity event graph.

When viewing the details of an EDR incident, you can determine the potential threat status by looking at the detection processing status. The application displays this status for the threat development chain. The background color for the status depends on the result of the threat detection object processing:

- If a detected threat is considered eliminated after being processed (for example, an infected object has been disinfected by an EPP application), the application displays the detection processing status on a green background;
- In all other cases, the detection processing status is displayed on a red background.

A key activity event in the activity event graph has the same color as the detection processing status.

If the detection processing status is displayed on a red background, you can prevent further development of a possible threat, for example, by triggering a response action in Kaspersky Industrial CyberSecurity for Networks.

Under any circumstances and regardless of the displayed detection processing status, you must investigate the causes and possible consequences of an EDR incident that has occurred.

You can view detailed information on activity events in the details windows that open when you select activity events. When viewing the details, you can use links with file and URL hashes to obtain information on the reputation of these objects on the Kaspersky Threat Intelligence Portal.

If the threat development chain contains activity events that you want to detect during the next checks of EPP applications, you can export the data on these activity events to an IOC file ? (an indicator of compromise ? file).

Creating allow rules for events

If you need to disable registration of events with specific indicators (for example, all events from a monitoring point), you can create allow rules for events.

Only users with the Administrator role can create allow rules for events.

You can use the following capabilities to create allow rules for events:

- **Create a rule with initially empty values of settings or with the values from a template.** ?

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. In the **Allow rules** section, open the details area by clicking the **Add rule** link.

3. If you want to define the values of settings from a template, in the details area click the **Use template** button, select the necessary template in the opened window and click **Apply**.

4. In the details area, click **EVT**.

5. In the **Protocol** field, specify the protocol that will be indicated in events.

   When the **Protocol** field is selected, a window opens showing the table of supported protocols displayed as a protocol stack tree. You can manage how tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   If necessary, use the search field above the table to find relevant protocols.

   To specify the protocol:

   a. In the protocols table, select the protocol that you want to specify for the rule. To select the relevant protocol, click the button that is displayed in the left column of the protocols table.

   b. Click **OK**.

   If you select a protocol that can be identified by the application based on the contents of network packets, a notification about this appears under the **Protocol** field.

6. If necessary, enter additional information about the rule in the **Comment** field.

7. In the **Side 1** and **Side 2** settings groups, specify the editable address information for the participants (sides) of network interaction. Depending on the selected protocol (or set of protocols), address information may contain a MAC address, IP address, and/or port number. If additional address spaces were added to the application, you can specify the names of the address spaces for addresses.

   To autofill the address information of a side of network interaction, you can select devices that are known to the application. To do so:

   a. Open the device selection window by clicking the **Specify device addresses** link.

   b. In the device selection window, select the check boxes next to the devices that you want to use.

      The device selection window contains a table in which you can configure the layout and order of columns, and filter, search, and sort similarly to the devices table in the **Assets** section.

   c. Click **OK** in the device selection window.

8. In the **Event type** field, specify the event type whose numerical code is indicated in events.

   Selecting the **Event type** field opens a window containing a list of event types that may be indicated in allow rules. If necessary, use the search field above the list to find the relevant event type. To specify the event type, select it in the list and click **Apply**.

9. In the **Monitoring point** field, specify the monitoring point name that is indicated in events.

   Selecting the **Monitoring point** field opens a window containing a list of all monitoring points on all nodes that have application components installed. If necessary, use the search field above the list to find the name of the relevant monitoring point. To specify the monitoring point name, select it in the list and click **Apply**.

10. In the **Rule in event** field, enter the name (or part of the name) that is indicated as the triggered rule in events.

11. In the details area, click **Save**.

    The new rule will be added to the allow rules table.

- Create a new rule based on an existing rule.

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. In the **Allow rules** section, select the rule that you want to use as the basis for creating a new rule.

3. Right-click to open the context menu.

4. In context menu select **Copy rule**.

   The details area in rule editing mode will appear in the right part of the web interface window. The settings of the new rule will take the values obtained from settings of the selected rule.

5. Change the settings as necessary. To do so, complete steps 4–11 described in the procedure for creating a rule with initially empty values of settings.

- Creating a rule based on a registered event

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.

2. Select the **Events and incidents** tab in the **Events** section.

3. In the table of registered events, select the event that you want to use as the basis for creating the allow rule for events.

   The details area appears in the right part of the web interface window.

4. In the details area, click the **Create allow rule** button.

   The **Allow rules** section opens in the browser window. The details area in rule editing mode will appear in the right part of the web interface window. The new rule's settings will take the values received from the saved information about the event.

5. If necessary, edit the settings of the new rule. To do so, complete steps 4–11 described in the procedure for creating a rule with initially empty values of settings. If you do not need to change the settings of the new rule, save the rule by clicking the **Save** button.

Setting markers

You can assign specific markers to events and incidents in the **Events** section of the application web interface.

A *marker* is an icon that lets you easily find events and incidents based on a criterion that is absent from the table.

To set a marker for an event or incident:

1. On the **Events and incidents** tab in the **Events** section, left-click to open the context menu in the cell of the **Marker** column for the row containing the relevant event or incident.
2. In the context menu, select the marker that you want to set for this event or incident.

   You can select one of the seven markers provided in the application. You choose the purpose of each marker on your own.
3. If you need to remove a marker, select **No marker** in the context menu.

Copying events to a text editor

You can copy information about the events and incidents displayed in the events table to any text editor. The information is copied from the columns that are currently displayed in the table.

The capability to copy is available if no more than 200 events and incidents are selected.

To copy events and/or incidents to a text editor:

1. Select the **Events and incidents** tab in the **Events** section.
2. In the events table, select the events and/or incidents whose information you want to copy to a text editor.
3. Right-click to display the context menu of one of the selected events.
4. In the context menu, select one of the following options:
   - **Copy details of the event** if one event or incident is selected.
   - **Copy details of the selected events** if multiple events and/or incidents are selected.
5. Open any text editor.
6. Paste it into the text editor window (for example, by pressing the key combination `CTRL+V`).

The copied event details can be edited in the text editor. Information about multiple events will be separated by an empty line.

Loading traffic for events

When viewing the events table, you can load traffic associated with registered events and/or incidents. Traffic is loaded into a PCAP file (when one event is selected) or into a ZIP archive containing PCAP files (when multiple events or incidents are selected).

The capability to load traffic is available if no more than 200 events are selected in the events table (including events within incidents).

Traffic for events is loaded from the application database. The database saves traffic only when registering events for which traffic saving is enabled. The application can also save traffic in the database directly by requesting to load traffic using traffic dump files. These files are intended for temporarily saving traffic and are automatically deleted as more and more traffic is received from the industrial network (the frequency of file deletion depends on the amount of traffic received and the defined application data storage settings). To ensure that traffic is loaded, it is recommended to enable the saving of traffic for the relevant event types and configure the settings for saving traffic in the database in accordance with the rate of traffic and registration of events.

To load a traffic file for events and/or incidents:

1. On the **Events and incidents** tab in the **Events** section, select the events and/or incidents for which you want to download traffic.
2. Click the **Download traffic** button.
3. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Exporting activity event data into a file of indicators of compromise

When viewing details of EDR incidents, you can export data on activity events to an IOC file if you wish to detect such activity events during the next checks of EPP applications. You can use the received IOC file in IOC search tasks performed using Kaspersky Endpoint Agent.

To export activity event data to an IOC file:

1. On the **Events and incidents** tab in the **Events** section, select an EDR incident (the event marked with the **EDR** icon) that contains a threat development chain with the appropriate activity events.

   The details area appears in the right part of the web interface window.
2. In the details area, go to the **All activity events** tab and select the appropriate activity events.

   You can select activity events of the following types: **File creation**, **Starting a process** or **Registry change**.
3. Click the **Export to IOC file** button.
4. In the window that opens, select a condition for detecting indicators of compromise:
   - **OR (any IOC detected)** if you want the IOC search task to be triggered when any indicator of compromise from the IOC file is detected.
   - **AND (all IOCs detected)** if you want the IOC search task to be triggered when all indicators of compromise from the IOC file are detected.

5. View the information that will be exported to the IOC file.

   Export is only available if non-zero values of the counters are displayed for any of the **File creation**, **Starting a process** and **Registry change** settings. The **Non-exportable** parameter contains the number of selected activity events whose data cannot be exported to an IOC file.

6. Click the **Export** button.

7. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Creating a folder for exporting events to a network resource

You can export events and save a file with the exported events on a network resource of the Server computer. You can share a network resource by using the Network File System (NFS) protocol, which is employed to mount a shared network resource of another computer (such as an NFS server export point) in the local file system of the Server computer. The standard tools of the operating system can be used to create a folder and to mount a shared network resource.

> When using the NFS protocol, the rpcbind software package is activated in the operating system. Please keep in mind that cybercriminals may attempt to use this software package to conduct certain types of DDoS attacks. To eliminate an infiltration threat, the firewall must be properly configured. In the CentOS Stream operating system, you are advised to use the network security configuration application known as Firewalld.

Manually creating a folder and mounting a shared network resource

To create a folder for saving files to a network resource:

1. Open the operating system console.

2. Create a local folder for mounting the shared network resource. To do so, enter the following command:

   ```
   mkdir <full path to the local folder>
   ```

   For example:

   ```
   mkdir ~/nfsshare
   ```

3. After the folder is created, enter the following command for mounting a network resource:

   ```
   sudo mount -t nfs <name or IP address of the remote computer>:\
   <full path to the shared network resource>\
   <full path to the local folder>
   ```

   For example:

```
sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
```

4. Check the mount result by using the following command:

   ```
   mount | grep <full path to the local folder>
   ```

   For example:

   ```
   mount | grep ~/nfsshare
   ```

   If mounting was successful, you will see data containing the name or IP address of the remote computer, the name of the shared network resource, and the name of the parent folder.

Automatically mounting a shared network resource

To configure automatic mounting of a shared resource in the CentOS operating system:

Open the /etc/fstab file for editing with root privileges and add the following string to the text of the file:

```
<name or IP address of the remote computer>:<full path to the shared network resource>
<full path to the local folder> nfs defaults 0 0
```

For example:

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

Monitoring risks

Kaspersky Industrial CyberSecurity for Networks can detect risks that could affect resources of an information system. The application detects risks based on traffic analysis and received information on devices.

The detected risks may belong to the following categories:

- Vulnerability. This category includes detected vulnerabilities of devices.
- Configuration problems. This category includes risks affecting the secure operation of devices due to incorrect configurations and risks of data compromise when writing and reading configurations of devices.
- ICS security breach. This category includes risks of information security breaches in automated industrial control systems.
- Insecure network architecture. This category includes risks associated with the detection of insecure network interactions, devices, protocols, and software, risks from inactivity of authorized devices, and risks from the absence or improper operation of EPP applications on devices.

Each risk is scored on a scale from 0.0 to 10.0. The application calculates this numeric risk score value based on the available information about the device associated with the detected risk. When calculating a risk score, the application considers the level of importance of the device, and other risks associated with this device. A *base score* is used as the initial value for calculations. Base scores of risks in the Vulnerability category are determined according to the Common Vulnerability Scoring System (CVSS). All other risk categories utilize the base scores defined in the table of risk types.

Information about risks is uploaded to the database of detected risks on the Kaspersky Industrial CyberSecurity for Networks Server. The total volume of saved entries in the database cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for detected risks when configuring data storage settings on the Server node.

The contents of the database of detected risks are displayed in the **Risks** section of the application web interface. You can also view general information about the risks associated with devices in the **Assets** section on the **Devices** tab.

About risks in the Vulnerability category

Vulnerability risks are registered when the application detects vulnerabilities in monitored industrial network devices. A *vulnerability* is a defect or flaw in device hardware or software that a hacker could exploit to impact the operation of an information system or to gain unauthorized access to information.

The application detects vulnerabilities by analyzing available information about devices. The relevant information utilized to find a known vulnerability of a device is compared to specific fields in the *database of known vulnerabilities*. The database of known vulnerabilities is built in to the application. This database is created by Kaspersky experts who fill it with information about the latest or most frequently encountered vulnerabilities of devices in industrial networks.

The database of known vulnerabilities contains descriptions of vulnerabilities and descriptions of the devices affected by these vulnerabilities. This database also contains system security recommendations in the form of text or links to publicly available resources. Descriptions and recommendations from various sources are uploaded to the database of known vulnerabilities. These sources may be the manufacturers of devices or software, or various organizations specializing in industrial security. Descriptions and recommendations in the database are provided in English.

> After the application is installed, the initial preconfigured database of known vulnerabilities is used. You can keep the database up to date by installing updates.

Kaspersky Industrial CyberSecurity for Networks compares available device information with the specific fields in the database of known vulnerabilities that describe devices affected by vulnerabilities. To detect vulnerabilities, the application uses the following information about devices:

- **Hardware vendor**.
- **Hardware model**.
- **Hardware version**.
- **Software vendor**. If no software vendor data is detected in the device information, Kaspersky Industrial CyberSecurity for Networks uses the value of the **Hardware vendor** setting.
- **Software name**. If no software name is detected in the device information, Kaspersky Industrial CyberSecurity for Networks uses the value of the **Hardware model** setting.
- **Software version**.

In the database of known vulnerabilities, descriptions of devices are stored in the CPE (Common Platform Enumeration) language format. The application compares the available device information with these descriptions, automatically converting the information into the CPE language format.

For each vulnerability, the matching descriptions are provided in the details area of the risk in the **Matched CPE** section.

If the device information matches the corresponding fields in the database of known vulnerabilities, the application registers a Vulnerability risk and uploads information about the vulnerability to the database of detected risks.

The main parameter used to identify a vulnerability is its identification number in the list of Common Vulnerabilities and Exposures (CVE). This identification number is known as a *CVE ID*. If a vulnerability has not yet been assigned a CVE ID, it is identified by its identification number obtained from other publicly available resources containing vulnerability descriptions.

Kaspersky Industrial CyberSecurity for Networks lets you obtain the identifiers and links to vulnerability descriptions provided by the Russian Federal Service for Technical and Export Control (FSTEC) in the Information Security Threat Database (also known as the BDU). If downloaded vulnerability information contains this type of information from the FSTEC BDU, the application displays this information as its corresponding identifiers in the format BDU:<year>-<number>.

Scenario for implementing the continuous risk management process

Risk detection functionality lets you implement continuous (cyclical) management of risks in your information system. For risk management purposes, Kaspersky Industrial CyberSecurity for Networks provides information on detected risks that you can use to take the appropriate measures to eliminate or mitigate those risks.

The scenario for implementing the continuous risk management process consists of the following stages:

1. **Device inventory**

   This stage is implemented by using the device activity detection and device information detection methods (these methods must be enabled). During this stage, the application automatically detects new devices and updates the device information. If the industrial network contains devices that have not been detected automatically, you need to manually add them or import them from external projects.

   For all information that defines the classification and operating specifications of devices (such as information about the device model and software version), you must enable auto update in the settings of devices. If auto update of this information cannot be completed for some reason, this information should be manually updated.

2. **Risk detection through passive and active scanning**

   The application passively scans devices for risks, utilizing the available device information. The application also detects risks by analyzing network interactions in industrial network traffic. Risk detection is implemented using the risk detection method (this method must be enabled).

   You can also perform active polling of devices to quickly obtain information about these devices. When performing active polling of devices, you also can detect specific types of risks if the corresponding risk analysis methods are selected. To conduct active polling of devices, one or more **Active poll** connectors must be added to the application.

   Vulnerability risks are detected automatically after the application database of known vulnerabilities is updated or after adding or modifying device information used for comparison (for example, after the information about the device model and software version is saved).

3. **Assessment and classification of detected risks**

   The application calculates a score value for each detected risk. This score determines the severity level of the risk. Depending on the numerical value of its score, a risk may have a *Low* (score of 0.0–3.9), *Medium* (4.0–7.9), or *High* (8.0–10.0) severity.

You can classify detected risks based on their severities and scores, and also on other factors related to the operational specifics of the devices used in your information system. If you assess a risk as negligible, its status can be manually changed from the *Active* status (assigned to a detected risk by default) to the *Accepted* status. For instance, this could be necessary if the conditions for exploiting a vulnerability cannot be reproduced anyway. When changing the status of a risk, it is recommended to add or edit the comment for the risk.

All risks that require some additional actions should be left with the *Active* status.

4 **Risk mitigation**

At this stage, you need to take actions that help either eliminate the detected risks or minimize the threats associated with the potential realization of these risks. To do so, check all detected risks that have the *Active* status, beginning with the risks that have the highest scores. Perform the necessary actions in your information system (for example, to eliminate a device vulnerability, install the required software update or isolate this device from external networks if the update is impossible). Information about recommended mitigation measures is provided for certain risks (such as vulnerabilities).

> Remediation actions for detected risks are performed without the involvement of Kaspersky Industrial CyberSecurity for Networks.

5 **Verification of risk mitigation**

This stage is similar to risk detection through scanning. When this stage is completed, the risks table should no longer have any *Active* status risks.

Most risks detected by the application during passive scanning (such as vulnerabilities) are automatically assigned the *Remediated* status if the conditions under which these risks were detected are no longer met. For example, after the version of software on a device is changed, the application assigns the *Remediated* status to a Vulnerability risk that had been registered due to a previous vulnerable version of the software. The *Remediated* status is also assigned to risks that no longer have a description in the database of known vulnerabilities (for instance, if the description is deleted from the database after updates are uploaded).

When deleting devices, the application also deletes the risks that were associated with these devices.

If you have taken action to mitigate a risk but the risk detection conditions have not changed (for example, a vulnerable device has been isolated from external networks but the information about this device has not changed), you can manually assign the *Accepted* status to this risk. When changing the status of a risk, it is recommended to add or edit the comment for the risk.

Some risks cannot be automatically assigned the *Remediated* status (for example, the *Remediated* status cannot be assigned to risks that are detected during active polling of devices). For these types of risks, you also have to manually assign the *Accepted* status after conducting risk mitigation measures.

If a risk is associated with an event, you can assign the *Accepted* status to this risk simultaneously while changing the event status to *Resolved*.

Viewing the risks table

The risks table is displayed in the **Risks** section of the application web interface.

The risk settings are displayed in the following columns of the table:

- **Category**

  Name of the risk category.

- **Name**

Name of the risk. The CVE ID of the detected vulnerability is used for a Vulnerability risk (if it has no CVE ID, it is identified by its identification number obtained from other publicly available resources containing vulnerability descriptions).

- **CVE**

  For a Vulnerability risk: CVE ID of the detected vulnerability.

- **BDU**

  For a Vulnerability risk: vulnerability ID in the BDU database. If one vulnerability with a CVE ID matches multiple vulnerabilities with different IDs in the BDU database, this column contains all the IDs.

- **Risk ID**

  Unique ID of the risk.

- **Score**

  Calculated value of the risk assessment. The severity of the risk is designated by a numerical score. Depending on the severity, the score may have one of the following colors:

  - Red designates a *High* severity risk.
  - Yellow designates a *Medium* severity risk.
  - Blue designates a *Low* severity risk.

  For risks with the *Active* status, the score is brightly colored. For *Remediated* or *Accepted* risks, its score is faintly colored.

- **Side 1**

  Address information of one of the sides of network interaction (indicated for certain risk types). MAC addresses and IP addresses can be individually enabled and disabled. If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the devices table.

- **Side 2**

  Address information of the other side of network interaction (indicated for certain risk types). The display of address information can be configured the same way as the **Side 1** column.

- **Device group**

  Name of the group containing the device with the detected risk (contains the name of the group and the names of all its parent groups).

- **Device**

  Device name and address.

- **Source of vulnerability**

  For a Vulnerability risk: name of the source of the information uploaded to the database of known vulnerabilities.

- **Status**

  Current status of the risk. The following statuses are available:

  - *Active* – default status upon first detection of the risk (and upon repeated detection if the *Remediated* status had been assigned to the risk). You can also manually assign the *Active* status to a risk if its current status is *Accepted*.

    - *Remediated* – automatically assigned status if the conditions for risk detection are no longer present.
    - *Accepted* – status manually assigned to a risk if the risk is assessed as negligible or if risk mitigation measures did not lead to automatic assignment of the *Remediated* status.

- **Detected**

  Date and time of risk detection.

- **Last status change**

  Date and time of the last change of the risk status.

- **Matched CPE**

  For a Vulnerability risk: descriptions of devices from the database of known vulnerabilities. These are descriptions that match device information in the devices table.

When viewing the risk table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing risk details

Risk details include information from the risks table and the following fields:

- **Risk type** – code of the risk type.
- **Description** – description defined for the risk type or the corresponding vulnerability.
- **Base score** – initial value used for calculating a numeric value for a risk score.

For a Vulnerability risk, additional information is displayed in the following fields and groups of fields:

- **CVSS vector** – record of metrics used to calculate a CVSS vulnerability score.
- **Attack conditions** – description of the vulnerability exploitation conditions.
- **Impact** – description of the potential effects from exploitation of the vulnerability.
- **Mitigations** – recommendations on remediating the vulnerability (for example, which software version should be installed on the device).
- **Links** – links to publicly available resources containing additional information about the vulnerability.
- **CVE history** – dates of identification, confirmation, and publication of the vulnerability in publicly available sources.

To view information about a risk:

Select the relevant risk in the risks table.

In the right part of the web interface window, you will see the area containing detailed information about the risk.

To view the details of a Vulnerability risk on the ***Devices*** *tab in the* ***Assets*** *section:*

Click the name of the vulnerability (displayed as a CVE ID or other identification number of the vulnerability) in the **Risks** column or in the details area of a device with this risk.

You will see a window containing detailed information about the vulnerability.

Manually changing the statuses of risks

When working in the **Risks** section, you can manually change the statuses of any risks with the *Active* status to the *Accepted* status and vice versa. When working in the **Assets** section, you can change the status only for Vulnerability risks and only from the *Active* status to the *Accepted* status.

You can also assign the *Accepted* status to a risk when assigning the *Resolved* status to events that are associated with this risk.

To manually change the status of a risk:

1. Open the risk details area or the window containing detailed information about the risk.
2. Open the **Change status** drop-down list.
3. Depending on the status you want to assign to the risk, select one of the following items in the drop-down list:
   - **Accepted** – if you want to change the risk status from *Active* to *Accepted*.
   - **Active** – if you want to revert the risk back to the *Active* status.

   A window with a confirmation prompt opens.
4. If events are associated with the selected risk and you want to simultaneously assign the *Resolved* status to all these events, select the **Assign the Resolved status to all related events** check box.

   Risks may be associated with events when the application registers events of certain types based on Asset Management technology.
5. In the prompt window, click **OK**.

Viewing risk details when working with the devices table

When working with the devices table you can view information about the risks that were detected on devices. The names of detected vulnerabilities (identified as CVE IDs or other identification numbers of the vulnerabilities) are displayed for each device that contains Vulnerability risks. If risks of other categories were detected on a device, the names of these risk categories are displayed for this device. The names of vulnerabilities and risk categories are displayed in the **Risks** column and in the details area when a device is selected.

By default, the devices table displays information only for the risks that are assigned the *Active* status. If necessary, you can enable the display of information about all risks by selecting the **Show remediated and accepted risks** check box when configuring the devices table.

To designate the severity levels of risks, the names of vulnerabilities and categories are displayed in one of the following colors:

- Red designates *High* severity risks.

- Yellow designates *Medium* severity risks.
- Blue designates *Low* severity risks.

For risks with the *Active* status, the names are brightly colored. For risks with the *Remediated* or *Accepted* status, the names are faintly colored.

If risks of the same category are associated with a device, the name of this category is shown in the color of the highest severity level of all these risks.

If you want to view detailed information about risks, you can use the displayed names of vulnerabilities and risk categories. Click the name of a vulnerability (displayed as a CVE ID or other identification number of the vulnerability) to open the details window of the vulnerability. When you click the name of a risk category, the application switches to the risks table and applies a filter to display risks of the selected category that are associated with the device.

When viewing the devices table, you can configure the settings for filtering devices based on their associated risks. You can also search for devices based on the names of their vulnerabilities (identified as CVE IDs or other identification numbers of the vulnerabilities).

Deep Packet Inspection

Kaspersky Industrial CyberSecurity for Networks lets you monitor an industrial process by providing you with information about the process parameters and system commands transmitted in industrial network traffic. The application tracks this data for devices that are displayed in the devices table and that have defined Process Control settings.

You can view the monitored tags and existing Process Control rules on the Server web interface page in the **Process control** section. The Process Control settings for devices are available when you select the corresponding devices in the **Assets** section and **Network map** section.

Monitoring process parameter values

Kaspersky Industrial CyberSecurity for Networks can display the values of process parameters (tags) in online mode.

To display these values, you must add the relevant tags to the application. You can add tags when configuring Process Control.

The application does not save the tag values displayed in online mode. The names and values of tags may be saved in events registered based on Deep Packet Inspection technology (the tag values received when the event is registered are saved in the event). To save the names and values of tags, the variable $tags must be present in the settings of event types.

To view the values of process parameters:

Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface and select the **Tags** tab in the **Process Control** section.

The browser window will display a table containing the tags and their current values. The following tag parameters show values that are modified on the fly:

- **Basic data type**.
- **Read/Write**.
- **Received**.
- **Timestamp**.
- **Timestamp status**.
- **Data status**.
- **Originator**.
- **Value**.
- **Structural values**.
- **Cause of transmission**.

To monitor the values of tags, you can utilize all the functions that are available when viewing the tags table.

Settings of tags

The settings of tags utilized for process control are displayed in the tags table and in the details area when a tag is selected.

Depending on the columns selected for display, the tags table may show the following settings:

- **Device group** – name of the group containing the device associated with the tag (contains the name of the group and the names of all its parent groups in the device group tree). In the details area, this setting is referred to as **Group**.
- **Device** – name of the device associated with the tag.
- **Protocol** – name of the protocol used to transmit the tag.
- **Tag name** – defined name of the tag.
- **Protocol data type** – tag data type indicating a specific name for the protocol operation (if such names are supported in the protocol, for example, for IEC 60870-5-104 and IEC 60870-5-101 protocols), or denoted by a standard data type name (for example, int32).
- **Unit of measure** – unit of measurement for the process parameter represented by the tag.
- **Basic data type** – data type for the value that is the primary value in the tag field structure (indicated by the standard data type name).
- **Read/Write** – direction of transmission when a tag value was received (R when reading from the device, W when writing to a device, and RW for both directions).
- **Favorites** – indicator of whether the tag was added to the favorites list.
- **Description** – additional information about the tag.

- **Tag address** – physical address of the tag in the device memory. In the details area, this setting is referred to as **Index**.
- **Tag ID** – sequential number of the tag. A tag ID is assigned automatically. In the details area, this setting is referred to as **ID**.
- **Received** – date and time when the tag value was last received by the application.
- **Timestamp** – date and time when the tag value (received from traffic) was last modified or updated.
- **Timestamp status** – current status for the date and time when the tag value was last modified or updated.
- **Data status** – current status of the received tag value.
- **Originator** – name of the source from which the tag value was received or the command was sent.
- **Value** – tag value that is modified on the fly during operations.
- **Scalable tag** – indicator of the tag scaling within the range of minimums and maximums for input and output values.
- **Input (minimum)** – minimum boundary of the input value.
- **Input (maximum)** – maximum boundary of the input value.
- **Output (minimum)** – minimum boundary of the output value.
- **Output (maximum)** – maximum boundary of the output value.
- **Structural values** – list of names and values of all tag fields. List items are separated by a comma and space (for example: `field1: <value1>, field2: <value2>`). The names of nested fields are generated from the names of all parent fields and the name of the actual field, separated by colons (for example: `parent1:parent2:field: <value>`). String values must be enclosed in quotation marks.
- **Cause of transmission** – reason for modification or transmission of the tag value (received from traffic).
- **Origin** – information about the source of tag creation. When a tag is automatically created using the Intrusion Detection technology, the **Origin** parameter is set to **System**. If the tag is created or modified by a user, the **Origin** parameter is set to **User**.

The details area for the selected tag may also display other settings determined by the device and protocol (for example: **Block number** and **Memory area**).

> The types of frames comprising application service data units (ASDU) are supported for Deep Packet Inspection on devices that interact over protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards. For information on the supported ASDU types identification in these protocols, please refer to the Appendices.

Viewing the tags table

The tags table is displayed on the **Tags** tab in the **Process control** section. The table provides the general parameters of tags and of the devices associated with the tags.

When viewing the tag table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Detecting default passwords when connecting to devices

When monitoring the communications of process control devices, Kaspersky Industrial CyberSecurity for Networks can determine when default passwords are used. If a connection is made to a device using a password that is set as the default password for the particular type of device, the application registers the corresponding event. To register default password detection events, the application uses the system event type for the detection of system commands.

Kaspersky Industrial CyberSecurity for Networks detects default passwords in the following cases:

- An attempt to use a default password was successful or the result of that attempt was not determined. In this case, an event is registered for the detection of the DEFAULT PASSWORD ENTRY system command.
- A new password matching the default password is set. In this case, an event is registered for the detection of the DEFAULT PASSWORD SET system command.
- The default password is received when reading the connection account credentials from a device. In this case, an event is registered for the detection of the DEFAULT PASSWORD READ or DEFAULT PASSWORD READ WITH TYPE system command (if the password details indicate its type, which determines the operations that can be performed with the device using this password).

Detection of default passwords is supported for certain types of devices and application-level protocols (see the table below).

Supported devices and protocols with default passwords

Devices	Protocols	System commands
ABB Relion series: RED670, REL670, RET670	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET
BECKHOFF® CX series	BECKHOFF ADS/AMS	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
Emerson ControlWave series	Emerson ControlWave Designer	DEFAULT PASSWORD ENTRY
General Electric Multilin series: B30, C60	Modbus TCP	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD READ WITH TYPE DEFAULT PASSWORD SET
Mitsubishi System Q E71	Mitsubishi MELSEC System Q	DEFAULT PASSWORD SET
Schneider Electric Modicon: M580, M340	Modbus TCP	DEFAULT PASSWORD READ WITH TYPE
Siemens SIMATIC S7-200, S7-300, S7-400	Siemens Industrial Ethernet Siemens S7comm	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ
Siemens SIMATIC S7-1200, S7-1500	Siemens Industrial Ethernet Siemens S7comm-plus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
PLC with the runtime system for CODESYS V3 (for example, Prosoft-Systems Regul R500)	CODESYS V3 Gateway	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET

EKRA 200 series	Modbus TCP for EKRA 200 series devices	DEFAULT PASSWORD READ DEFAULT PASSWORD SET
EKRA BE2502, BE2704 series	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET

To register default password detection events, the following conditions must be met:

- Interaction Control is enabled in monitoring mode and Command Control technology is applied.
- The allow rules table does not contain any rules for Command Control technology that allow system commands with default passwords. For example, the application may automatically create these rules in Interaction Control learning mode. If these rules are present in the allow rules table, you are advised to disable them.
- For the relevant devices, tracking of system commands with default passwords is enabled.

Obtaining reports

In Kaspersky Industrial CyberSecurity for Networks, you can generate reports based on templates to obtain information about devices, the statuses of devices and system security, monitored technological process parameters and system commands, and information about detected risks and interactions with third-party devices.

The application has two types of report templates:

- System templates are created automatically during installation of the application. In the report templates table, system templates are displayed with the 🛡 icon. You cannot delete system templates.

  Kaspersky Industrial CyberSecurity for Networks supports the following system templates for generating reports:

  - **Inventory report**.

    Report containing information about devices, monitored technological process parameters and system commands, utilized protocols, and detected risks on devices.

  - **System security report**.

    Report containing information about the security status of devices, registered events, detected risks, and interactions with devices of external networks.

  - **Executive summary**.

    Report containing concise information about devices and the security status of the system.

  - **Full report**.

    Report containing comprehensive information about devices and the security status of the system.

- User-defined templates are created manually by duplicating templates. System templates and user-defined templates can be duplicated. Only users with the Administrator role can duplicate templates.

Data in reports is presented in separate information blocks. For each report, Kaspersky Industrial CyberSecurity for Networks uses a fixed set and layout of information blocks. The information blocks used in reports and their descriptions are presented in the table below.

Use of information blocks in reports

Name of information block	Inventory	System security	Executive	Full

	report	report	summary	report
Device categories	✓	—	✓	✓
Device vendors	✓	—	✓	✓
Device operating systems	✓	—	✓	✓
Monitored technological process parameters	✓	—	—	✓
Devices with the most risks	✓	✓	—	✓
Most vulnerable industrial devices	✓	✓	—	✓
System command sources	✓	—	—	✓
Situational awareness	—	✓	✓	✓
New devices in the network	✓	—	—	✓
Protocols with the most traffic	✓	—	—	✓
Devices with the most connections to other nodes	✓	—	—	✓
Network traffic volume	✓	—	✓	✓
Common protocols	✓	—	✓	✓
Industrial protocols	✓	—	✓	✓
System command recipients	✓	—	—	✓
Device security statuses	—	✓	✓	✓
Distribution of devices by status	—	✓	—	✓
Statistics on events	—	✓	—	✓
Distribution of events by detection technologies	—	✓	—	✓
Devices with the most events	—	✓	—	✓
Most critical events	—	✓	—	✓
Most frequently triggered malicious activity detection rules	—	✓	—	✓
Unusual protocols in the industrial network	—	✓	—	✓
Devices with signs of access to public resources	—	✓	—	✓
Connections via remote control protocols	—	✓	—	✓
Modification of industrial device programs	—	✓	—	✓
Active risks	—	✓	✓	✓

You can manually start generating reports based on templates in the **Reports** section on the **Report templates** tab of the application web interface. Kaspersky Industrial CyberSecurity for Networks can also start generating reports according to a schedule. Only users with the Administrator role can configure template schedule settings.

Kaspersky Industrial CyberSecurity for Networks generates reports in PDF files that are no more than 10 MB in size, and sends the report files to the email addresses indicated in the report templates. You can view information about generated reports and export them to files on the **Generated reports** tab.

The **Generated reports** tab also displays the reports generated when working with security audit jobs. A user with the Administrator role starts **generation of reports** with the results of device scans as part of a security audit job, as well as reports on the starts of the security audit job in the Security audit section.

Viewing the report templates table

You can view the report templates table in the **Reports** section on the **Report templates** tab of the application web interface.

The settings of report templates are displayed in the following columns of the table:

- **Name**.

  Report template name. The 🛡 icon is displayed next to the names of system report templates.

- **Schedule**

  Information about the schedule used by Kaspersky Industrial CyberSecurity for Networks to automatically generate a report based on the template. Schedule information is displayed if a user with the Administrator role configured the schedule settings in the report template. If schedule settings were not defined, the **Disabled** value is displayed in the column.

- **Type/user**.

  Name of the user who last modified the report template. The **System** value is displayed for system templates that have the default settings.

- **Last report**.

  Date and time when report generation was last started based on the report template.

- **Destinations**.

  This icon indicates that there are email recipients of reports. The following icons are provided:

  - ✉ – report recipients are defined.
  - ✉ – report recipients are not defined.

When viewing the report templates table, you can use the configuration and sorting functions.

Viewing report template details

To view information about a report template:

On the **Report templates** tab in the **Reports** section, select the relevant template.

The details area appears in the right part of the web interface window. The details area displays all data that has defined values.

Report template details include the following fields:

- **Name** – report template name.

- **Type/user** – name of the user who last modified the report template. The **System** value is displayed for system templates that have the default settings.
- **Period** – time period covered when Kaspersky Industrial CyberSecurity for Networks generates a report based on the template.
- **Modified** – time of the most recent change to the template.
- **Last report** – time when the last report was generated based on the template.
- **Next start (local time)** – time when the next report generation will start based on the template. This setting is displayed if schedule settings were defined for the report template.
- **Schedule** – information about the schedule used by Kaspersky Industrial CyberSecurity for Networks to automatically generate a report based on the template. This setting is displayed if schedule settings were defined for the report template.
- **Recipient addresses** – email addresses to which Kaspersky Industrial CyberSecurity for Networks sends the generated reports. This setting is displayed if recipient addresses were defined for the report template.

Manually generating a report

You can manually start report generation based on a template. Report generation can be manually started by users with the Administrator role and users with the Operator role.

To start generating a report:

1. Select the **Reports** section.
2. On the **Report templates** tab, select one or more templates that you want to use to generate reports.

   When multiple templates are selected, the application simultaneously generates reports based on them. You can select no more than 10 templates.
3. Click the **Get reports** button in the toolbar located above the report templates table.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process. If necessary, you can contact a user with the Administrator role to cancel report generation.

You will be taken to the **Generated reports** tab, which will display the completion status of the reports being generated. After the reports are generated, Kaspersky Industrial CyberSecurity for Networks sends the report files in PDF format to the email addresses indicated in the report template. If an email address is not defined in the report template, you can individually export generated reports to files manually on the **Generated reports** tab. The maximum size of a report file is 10 MB.

Viewing the reports table

You can view the reports table in the **Reports** section on the **Generated reports** tab of the application web interface.

The report settings are displayed in the following columns of the table:

- **ID**

  Unique identifier of the report.

- **Report name**.

  Name of the generated report.

- **Template name**.

  Name of the template used to generate the report.

- **Start**.

  Date and time when report generation was started.

- **Status**

  Report completion status. The following report completion statuses are provided:

  - *Waiting*. The report is in the creation queue. A report may have the *Pending* status when multiple reports are being generated at the same time.
  - *In progress*. The report is currently being generated.
  - *Error*. An error occurred when generating the report.
  - *Done*. Report generation is complete.
  - *Canceling*. Report generation is being canceled.
  - *Canceled*. Report generation was canceled.

- **User**

  Name of the user who started report generation or configured the schedule for generating a report based on a template.

- **Run type**.

  Type of report generation launch: manually or as scheduled.

- **Completed**.

  Date and time when report generation completed.

When viewing the reports table, you can use the configuration, filter, and sorting functions.

Exporting a report to a file

You can export a generated report to a file in PDF format.

To export a report to a file:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select the relevant report.

   Reports are filtered based on the IDs of reports that were last run in the current Server connection session. To display all generated reports, reset the filter settings by clicking the **Default filter** button. If necessary, you can configure filtering based on a specific period of time.

   The details area appears in the right part of the web interface window.
3. Click the **Export** button.

The browser will save the report file. By default, a report file is named according to the format `<report name>_<report generation date and time>`. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Detecting security issues in encryption protocols

If encryption protocols (such as SSL/TLS or SSH) are being used in an industrial network, Kaspersky Industrial CyberSecurity for Networks can detect various security issues in network interactions using these protocols. The application registers the appropriate event when detecting a security issue. The system event type for the detection of system commands is used to register these events.

The application registers events when it detects the following security issues in an encryption protocol:

- Use of an outdated version of an encryption protocol (DEPRECATED PROTOCOL VERSION).
- Use of a weak encryption algorithm (WEAK CIPHER TYPE).
- Use of an expired certificate (OUTDATED CERTIFICATE).
- Use of a self-signed certificate (SELF-SIGNED CERTIFICATE).

The list of detected security issues depends on the specific encryption protocol.

> After installation, the application uses the original protocol processing modules that support a limited number of encryption protocols. You can update protocol processing modules by installing updates.

You do not need to add Process Control settings for devices to detect security issues in encryption protocols. The application analyzes the encryption protocols in all detected interactions.

To register security issue detection events, the following conditions must be met:

- Interaction Control is enabled in monitoring mode and Command Control technology is applied.
- The allow rules table does not contain any rules for Command Control technology that block the registration of events regarding security issues in encryption protocols. For example, the application may automatically create these rules in Interaction Control learning mode. If these rules are present in the allow rules table, you are advised to disable them.

Typical actions when working with data tables

This section contains information about the typical operations performed when working with the data tables that are displayed in different sections of the application web interface (such as the devices table, events table, or tags table).

Viewing a data table

When viewing data tables in different sections of the application web interface, you may be able to use the following functions:

- Configuring the columns display and order

  Depending on the specific section of the application web interface, you can enable and disable the display of specific data in the table and configure which columns to display and in which order.

  To configure the table display settings:

  1. Click the ⚙ icon to open the window for configuring how the table is displayed.
  2. If enabling and disabling the display of specific data is available for the table (for example, display of remediated and accepted risks in the devices table), configure the settings in the upper part of the window.
  3. In the **Displayed columns** settings group, select the check boxes opposite the settings that you want to view in the table. You must select at least one setting.
  4. If you want to change the order in which columns are displayed, select the name of the column that needs to be moved to the left or right in the table and use the buttons containing an image of the up or down arrows.

  The selected columns will be displayed in the table in the order you specified.

- Filtering based on standard time periods

  1. When working with a table in a section of the application web interface, open the **Detection period**, **Run period** or **Period** drop-down list in the toolbar.
  2. In the drop-down list, select one of the standard periods (for example, **Last 24 hours**).

  The table will display data for the period you specified.

- Filtering based on a specified time period

1. In a table of the application web interface section, on the toolbar, open the **Period**, **Detection period**, or **Run period** drop-down list.

2. In the drop-down list, select **Specify a period**.

   The start and end date and time of the filtering period are displayed on the right of the drop-down list.

3. Click the date of the start or end of the period.

   The calendar opens.

4. In the calendar, specify the date for the start and end boundaries of the filtering period. To do so, select a date in the calendar (the current time will be indicated) or manually enter the value in the format DD-MM-YYYY hh:mm:ss. If you do not need to specify the date and time of the filtering period end boundary, you can choose not to select a date or you can delete the current value.

5. Click **OK**.

The table will display data for the period you specified.

- Filtering by columns ?

To filter a table by a specific column:

1. In a table of a section of the application web interface, click the filtering icon in the relevant column.

   The filtering window opens.

2. Use the interface elements in the filter window to configure the settings, as necessary. Below are some special considerations when configuring a filter in certain columns.

3. Click **OK**.

If the filter window contains the **Complex** parameter

Use the **Complex** parameter to specify multiple values combined by the logical operator AND. To add different types of values, use the **Add condition (AND)** button.

If there is a column for groups of devices

1. In the filter window, click the icon in the right part of the field to select a group.

   The **Select group in tree** window appears.

2. In the device group tree, select the relevant group and click the **Select** button.

   The path to the selected group is displayed in the field in the filter window.

If there is a column for risks associated with devices

1. In the filter window, use the **Exclude devices with risks** toggle button to configure the display of devices in the table:

   - To view only risk-free devices, turn on the toggle button.

   - To view the devices with risks and to configure the settings for filtering by risk, turn off the toggle button.

2. If necessary, use the following controls to configure the settings for filtering devices with risks:

   - **Risk scores** – lets you define a range of risk score values for displaying devices with risks whose scores are within the specified range.

   - **Status** – groups buttons for enabling and disabling filtering based on the statuses of risks (the buttons are displayed if the **Show remediated and accepted risks** check box is selected in the devices table display settings).

If there is a **Protocol** column displaying supported application-layer protocols

1. In the filter window, specify the necessary protocol in the **Protocols** field. To do so, start entering the name of the protocol and select the relevant protocol from the drop-down list (the list of suitable protocols is automatically expanded when the value in the **Protocols** field is changed).

2. If necessary, sort the opened list of protocols by clicking the **Sort** link.

3. If you want add another protocol, click the **Add protocol** button and specify the other protocol in the opened field.
4. If you want to delete one of the specified protocols, click the 🗑 icon in the filter window. You can also delete all specified protocols by clicking the **Default filter** link in the filter window.

If there is a **Protocol** column that displays all supported protocols in the form of a protocol stack tree

1. In the filter window, configure how the relevant tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   The table columns provide the following information:

   - **Protocol** – name of the protocol within the protocol stack tree.
   - **EtherType** – number of the next-level protocol within the Ethernet protocol (if the protocol has a defined number). It is displayed in decimal format.
   - **IP number** – number of the next-level protocol within the IP protocol (if the protocol has a defined number). It is indicated only for protocols within the IP protocol structure. It is displayed in decimal format.
2. If necessary, use the search field above the table to find relevant protocols.
3. In the list of protocols, select the check boxes opposite the protocols by which you want to filter events.

   If you select or clear the check box for a protocol that contains nested protocols, the check boxes for the nested protocols are also automatically selected or cleared.

If filtering based on the table cell values is allowed

1. Select the relevant items in the data table.
2. Move your mouse cursor over a cell of the relevant column of one of the selected items.
3. Right-click to open the context menu.
4. In the context menu, select the command that shows all items containing the specific value or values of a parameter.

Modes for filtering events within incidents

When filtering the events table in tree display mode, incidents that meet the filtering criteria may be presented in the following variants:

- Displayed with all nested elements
- Displayed only with the nested elements that also meet the defined filtering criteria

You can select the relevant display option for incidents by using the **Show embedded events when filtering** check box when configuring the table.

- Table search

  In a table of a section of the application web interface, you can find relevant items by using the **Search <type of displayed items>** field. The field is displayed in the right part of the section.

  A search can be run on selected table columns.

- Resetting the defined filter and search settings

  In a table of a section of the application web interface, you can reset the defined filter and search settings by using the **Default filter** button in the toolbar. The button is displayed if search or filter settings are defined.

- Table sorting

  1. In a table of a section of the application web interface, click the header of the column by which you want to sort.

     The headers of columns that can be sorted are displayed as links.

  2. If sorting is performed based on a column that displays different types of values (for example, the **Side 1** column in the **Risks** section)**,** use the drop-down list of the column header to select the parameter that will be used for sorting.

  3. If you need to sort the table based on multiple columns, press the `SHIFT` key and hold it down while clicking the headers of the columns by which you want to sort.

  The table will be sorted by the selected column. When sorting by multiple columns, the rows of the table are sorted according to the sequence of column selection. Next to the headers of columns used for sorting, you will see icons displaying the current sorting order: in ascending order or descending order of values.

Selecting elements in a data table

In a table of a section of the application web interface, you can select any displayed items to view their details and to manage these items. When you select an item in the table, you will see the details area in the right part of the web interface window.

To select the relevant items in the table, do one of the following:

- If you want to select one item, select the check box on the left side of the row containing this item or use your mouse to select the table row.

- If you want to select multiple items, select the check boxes on the left side of the rows containing the relevant items, or select them while holding down the `CTRL` or `SHIFT` key.

- If you want to select all items that satisfy the current filter and search settings, do one of the following:

  - Select any item in the table and press the key combination `CTRL+A`.

  - Select the check box in the title of the left-most column of the table.

If multiple items are selected, data on their number is displayed in the upper-right corner of the web interface page. The precise number of selected items is displayed up to a specific limit (for example, up to 2,000 items). If more items are selected, the precise number is not displayed (in the above example, `2,000+` will be displayed). If no items are selected in the table, the total number of items in the data table is displayed in the upper-right corner of the page.

The header of the left-most column of the table shows the item selection check box. Depending on the number of selected items, the check box can have one of the following states:

- □ – all items that satisfy the current filter and search settings were not selected in the table. In this case, one item or multiple items may be selected in the table by using the check boxes on the left side of rows or by using the **`CTRL`** or **`SHIFT`** key.
- ☑ – all items that satisfy the current filter and search settings are selected in the table.
- ▣ – all items that satisfy the current filter and search settings were selected in the table, but then the check boxes for some of the items were cleared. This state is also retained if the check boxes were cleared for all items selected in this way (due to the fact that the number of selected items may change).

> If all items that satisfy the filter and search settings are selected, the number of selected items may automatically change. For example, this could occur as a result of the user's actions in another connection session or when new items are discovered. You are advised to configure the filter and search settings so that you only see the relevant items in the selection.

Navigating to related items in other web interface sections

Items in certain sections of the application web interface (in particular, in data tables) can be associated with the items in other sections containing tables or data structures. For example, events may be related to devices or to risks. When working with such items, you can navigate to the related items in other sections to view details.

To view information about related items:

1. Select the items for which you want to view information about the related items.

   It is recommended to select a limited number of items (up to 200). When you select a large number of items, you may not be able to navigate to view the related items.

2. Open the **Show related** drop-down list in the toolbar.

3. In the drop-down list, select the desired item type (for example, **Devices**).

A section opens that contains the items of the selected type (in this example, the devices table in the **Assets** section). The corresponding filtering is applied to display related items.

Exporting data from a table to a file

The data tables of certain sections of the application web interface provide the capability to export data to files in the following formats:

- CSV

When exporting to this format, the file saves information from the columns currently displayed in the table. Certain data that is not displayed in the table (for example, additional fields and Process Control settings in device information) may also be stored in this format.

- JSON

  When exporting a file in this format, all the data for table items is saved, including service information from the database (such as information about events associated with the devices).

You can export information for all items that satisfy the current filter and search settings, or selectively for items displayed in the table.

To export data for all items that satisfy the current filter and search settings:

1. Click the **Export** link on the toolbar above the data table to open the menu and select the item with the desired file format: CSV or JSON.

2. If the option to save supplementary settings is available for export, in the window that appears, select the check boxes for the settings that you want to export.

   The file creation process starts.

3. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the ⤓ button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file creation operation to finish.

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

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

To export data for the selected items:

1. Select the items whose information you want to export to a file.

2. Right-click to display the context menu of one of the selected items.

3. In the context menu, select the relevant file format option: CSV or JSON.

4. If the option to save supplementary settings is available for export, in the window that appears, select the check boxes for the settings that you want to export.

   The file creation process starts.

5. If it takes a long time (more than 15 seconds) to create the file, perform the necessary actions for step 3 as described in the procedure for exporting data for all items.

Updating a data table

The specific data displayed in a table of a section of the application web interface could possibly be changed on the Server while you are viewing the table (for example, when new items are registered or if data has been modified in a different session of connecting to the Server). Some tables support automatic data updates.

To enable or disable automatic update of data in a table:

On the toolbar above the data table, use the **Update** option.

Managing the application through Kaspersky Security Center

This section contains information about configuring interaction between the application and Kaspersky Security Center, and information about using Kaspersky Security Center functions for working with Kaspersky Industrial CyberSecurity for Networks. You can use Kaspersky Security Center to do the following:

- Add a license key to Kaspersky Industrial CyberSecurity for Networks.
- Download updates for application modules and databases to Kaspersky Industrial CyberSecurity for Networks.
- View Kaspersky Industrial CyberSecurity for Networks events in the Kaspersky Security Center Administration Console.
- Monitor the ICS security state in the Administration Console or in a SCADA system.
- Remotely connect to the Kaspersky Industrial CyberSecurity for Networks Server computer.
- Use advanced capabilities of centralized system monitoring with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console.
- Use Single Sign-On technology for authentication of Kaspersky Security Center Web Console users when they connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.

> The contents of the available actions list depends on the capabilities of the Kaspersky Security Center version at hand. You can view information about the key features of various Kaspersky Security Center versions in the Kaspersky Security Center Help System.

To enable interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center, the following conditions must be fulfilled:

- The functionality for application interaction with Kaspersky Security Center was added during installation of the Kaspersky Industrial CyberSecurity for Networks Server.
- In Kaspersky Industrial CyberSecurity for Networks, the functionality for interaction with Kaspersky Security Center has been enabled and configured.
- The Kaspersky Industrial CyberSecurity for Networks Administration Plug-in is installed in Kaspersky Security Center Windows.
- The Kaspersky Industrial CyberSecurity for Networks administration web plug-in is installed in Kaspersky Security Center Web Console for use in Kaspersky Security Center Linux, and to implement advanced centralized control and Kaspersky Security Center Windows single sign-on.
- The computer on which the Kaspersky Industrial CyberSecurity for Networks Server is installed is included in the Kaspersky Security Center administration group (in the **Managed devices** group or its subgroup). You can move the device to the administration group when working in the MMC-based Administration Console or when registering Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console.
- Certain ports and protocols used for connections and interactions between the Kaspersky Industrial CyberSecurity for Networks Server and the Kaspersky Security Kaspersky Security Center Administration Server or the Kaspersky Security Center Web Console are available.

Enabling and configuring interaction with Kaspersky Security Center

After the functionality for interaction with Kaspersky Security Center is added to the application, this functionality is disabled by default.

To enable and configure the functionality for application interaction with Kaspersky Security Center:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Kaspersky Security Center**.
3. Use the **Enabled** toggle button to enable interaction with Kaspersky Security Center.
4. In the **Connector settings** block, configure the settings of the **Kaspersky Security Center Connector**:
   - IP address / network name of the computer hosting the Kaspersky Security Center Administration Server.
   - SSL port for the connection.
   - Maximum number of relayed events per day, starting at 0:00 in the time zone of the Kaspersky Industrial CyberSecurity for Networks Server.
5. In the **Plug-in for Kaspersky Security Center Web Console** block, configure the settings for connections from the Kaspersky Security Center Web Console:
   - Kaspersky Industrial CyberSecurity for Networks user name that will be indicated in audit log entries when actions are registered from the Kaspersky Security Center Web Console.
   - IP address / network name of the web server.
   - IP address / network name of the REST API server.
6. Click the **Apply** button.

Adding a license key to Kaspersky Industrial CyberSecurity for Networks from Kaspersky Security Center

You can add a license key to Kaspersky Industrial CyberSecurity for Networks by using the functionality for automatic distribution of license keys to Kaspersky Security Center. A license key received in this way is processed in Kaspersky Industrial CyberSecurity for Networks the same as a license key that is added manually in the application.

Automatic license key distribution works if all conditions for communication between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center are met.

To distribute a license key, you need to first add it to the Kaspersky Security Center Administration Server repository. You can add the license key to the storage when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console. To add, use a license key file.

After adding the license key to the Administration Server repository, you can create a license key distribution task when working in the MMC-based Administration Console ↗ or when working in Kaspersky Security Center Web Console ↗.

Receiving updates from the Kaspersky Security Center Administration Server

You can use the Kaspersky Security Center Administration Server as the source of updates for databases and application modules of Kaspersky Industrial CyberSecurity for Networks. This method of receiving updates may be required if, for example, you need to download updates from Kaspersky servers when the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server has no Internet access.

The scenario for preparing the Kaspersky Security Center Administration Server for use as an update source consists of the following steps:

1. **Creating a task in Kaspersky Security Center to download updates to the Administration Server repository**

   You can create a task when working in the MMC-based Administration Console ↗ or when working in Kaspersky Security Center Web Console ↗.

2. **Selecting the Administration Server as an update source in Kaspersky Industrial CyberSecurity for Networks**

   When connected to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface, you can select the Kaspersky Security Center Administration Server as the update source when starting the update process manually and/or when configuring automatic updates.

Monitoring events via Kaspersky Security Center

In Kaspersky Security Center, information about events of Kaspersky Industrial CyberSecurity for Networks is displayed in the following columns of the events table:

- **Time** or **Event occurred** means the Kaspersky Industrial CyberSecurity for Networks event registration time in the time zone of the computer where Kaspersky Security Center is installed.
- **Device** means the name of the managed device in Kaspersky Security Center (the computer on which Kaspersky Industrial CyberSecurity for Networks Server is installed).
- **Event** means the name of the Kaspersky Security Center event type defined for events of Kaspersky Industrial CyberSecurity for Networks.
- **Description** means the title and brief description of the Kaspersky Industrial CyberSecurity for Networks event.
- **Group** or **Administration group** is the name of the administration group that contains the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server in the **Managed devices** folder in the Kaspersky Security Center Administration Console tree.
- **Application** means the application name (Kaspersky Industrial CyberSecurity for Networks).
- **Version number** means the application version number.
- **Importance** or **Severity** means the importance level of the event based on how importance is typified by Kaspersky Security Center.

- **Registered** or **Event registered** means the time at which the event was registered in the Kaspersky Security Center database.

The parameter values of events relayed from Kaspersky Industrial CyberSecurity for Networks are displayed according to the localization settings of Kaspersky Industrial CyberSecurity for Networks. The localization language of Kaspersky Security Center is disregarded for these parameters.

If a Kaspersky Industrial CyberSecurity for Networks event contains information about multiple network interactions, this event is converted into separate items of the Kaspersky Security Center events table. This way, individual events are created in Kaspersky Security Center for each network interaction specified in a Kaspersky Industrial CyberSecurity for Networks event.

To have events of Kaspersky Industrial CyberSecurity for Networks displayed in the Kaspersky Security Center events table:

1. Make sure that the required components are installed in Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center.
2. Make sure that the port used for connecting to the computer hosting Kaspersky Security Center is open and accessible on the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server.
3. When configuring the Network Agent policy settings in Kaspersky Security Center, enable saving of relevant events to the Administration Server database and define the event retention period.

   You can configure event registration and retention in the Network Agent policy settings when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console.
4. In Kaspersky Industrial CyberSecurity for Networks, configure forwarding of events through the **Kaspersky Security Center Connector**.

When the specific event types are registered in Kaspersky Industrial CyberSecurity for Networks, these events will also be displayed in the Kaspersky Security Center events table.

Event types in Kaspersky Security Center for Kaspersky Industrial CyberSecurity for Networks events

A fixed set of event types are used for receiving events of Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center. The event types in Kaspersky Security Center correspond to the specific event types in Kaspersky Industrial CyberSecurity for Networks and can be registered as Kaspersky Security Center incidents depending on the severities of the events (see the figure below).

Types of events in Kaspersky Security Center for receiving events of Kaspersky Industrial CyberSecurity for Networks

Displayed name of the event type	Code of the event type in Kaspersky Security Center	Registration as a Kaspersky Security Center incident	Corresponding event type code in Kaspersky Industrial CyberSecurity for Networks
Maximum number of reported events has been reached	32769	yes, with the *Warning* severity level	–
Test event (DPI)	32770	no	4000000001
Test event (NIC)	32771	no	4000000002
Test event (IDS)	32772	no	4000000003
Test event (AM)	32773	no	4000000004
Unauthorized network interaction detected	32774	no	4000002601
System command detected	32775	Only events with the	4000002602

		Critical severity level	
No traffic at monitoring point	32776	no	4000002700
TCP protocol anomaly detected: content substitution in overlapping TCP segments	32777	no	4000002701
Process Control rule violation	32778	Only events with the *Critical* severity level	4000002900
Intrusion Detection rule from the system set of rules was triggered	32779	no	4000003000
Intrusion Detection rule from the user-defined rule set was triggered	32780	no	4000003001
Symptoms of ARP spoofing detected in ARP replies	32781	yes	4000004001
Symptoms of ARP spoofing detected in ARP requests	32782	yes	4000004002
New device detected in network	32783	yes	4000005003
New device settings detected	32784	no	4000005004
IP address conflict detected	32785	yes	4000005005
Activity detected from device with Archived status	32786	no	4000005006
New IP address of device detected	32787	yes	4000005007
New MAC address of device detected	32788	yes	4000005010
MAC address added to device	32789	no	4000005008
IP address added to device	32790	no	4000005009
PLC Project Control: detected read of unknown block from PLC	32791	no	4000005200
PLC Project Control: detected read of known block from PLC	32792	no	4000005201
PLC Project Control: detected write of new block to PLC	32793	no	4000005202
PLC Project Control: detected write of known block to PLC	32794	no	4000005203
PLC Project Control: detected read of unknown project from PLC	32795	no	4000005204
PLC Project Control: detected read of known project from PLC	32796	no	4000005205
PLC Project Control: detected write of new project to PLC	32797	no	4000005206
PLC Project Control: detected write of known project to PLC	32798	no	4000005207
IP protocol anomaly detected: data conflict when assembling IP packet	32799	no	4000005100
IP protocol anomaly detected: fragmented IP packet size exceeded	32800	no	4000005101
IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	32801	no	4000005102
IP protocol anomaly detected: mis-associated fragments	32802	no	4000005103
Correlation rule event registered	32803	Only events with the *Critical* severity level	8000000001
Custom event based on External technology	32804	Only events with the *Critical* severity level	4000005400
Different MAC address of device detected in	32805	yes	4000005011

data received from EPP application			
New address information of device detected in data received from EPP application	32806	yes	4000005012
Conflict detected in device addresses after data received from EPP application	32807	yes	4000005013
Subnet added based on data from EPP application	32808	yes	4000005014
Device equipment change detected	32809	no	4000005015

Correspondence of Kaspersky Security Center event severity levels

Severity of events in Kaspersky Security Center correspond to the importance levels of Kaspersky Industrial CyberSecurity for Networks events (see the table below). For the severity levels of Kaspersky Industrial CyberSecurity for Networks events, the corresponding names of severity levels used in previous application versions are specified.

Correspondence between event severities

Kaspersky Security Center event severities	Kaspersky Industrial CyberSecurity for Networks event severities
Informational message	*Low* (*Informational*)
Warning	*Medium* (*Warning*)
Critical event	*High* (*Critical*)

Monitoring the ICS security state: Kaspersky Security Center and SCADA

Kaspersky Industrial CyberSecurity for Networks can relay data about the ICS security state to Kaspersky Security Center. To transmit data to Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center, the required components must be installed.

If the transmission of ICS security state data to Kaspersky Security Center has been configured, you can configure the SCADA system to receive the corresponding information from Kaspersky Security Center.

To configure a SCADA system to receive and display the ICS security state:

1. Install Kaspersky Security Gateway on the computer hosting Kaspersky Security Center.

   You can find detailed information on installing and configuring Kaspersky Security Gateway in the *Kaspersky Security Gateway Administrator Guide*.

2. In the SCADA system, create a control element that reflects the state of the computer with Kaspersky Industrial CyberSecurity for Networks.

3. Configure the created control element to receive data over the OPC DA 2.0 or IEC 60870-5-104 protocol.

   Instructions on configuring the control element are provided in the *Kaspersky Security Gateway Administrator Guide*.

Connecting to the Server computer from Kaspersky Security Center

You can remotely connect to the Kaspersky Industrial CyberSecurity for Networks Server computer from the Kaspersky Security Center Administration Console. This requires the use of the MMC-based Administration Console. The Virtual Network Computing (VNC) remote desktop access system is used to make the connection.

To connect, you must install and configure the following VNC components:

- VNC server. It is installed on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server. When configuring the VNC server, you need to set a password for the VNC connection. If a firewall is enabled on the computer, you also need to open the ports for the VNC and SSH protocols.
- VNC client. It is installed on the computer that has the Kaspersky Security Center Administration Console.

To gain access to the Kaspersky Industrial CyberSecurity for Networks Server computer from Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the computer on which the Kaspersky Industrial CyberSecurity for Networks Server is installed.
3. In the workspace on the **Devices** tab, select the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server, and select **External tools** → **VNC** in the context menu of the computer.

   By default, the VNC tool is absent from the list of external tools. To add the tool, in the context menu of the computer, select **External tools** → **Configure external tools**. In the **External tools** window, click the **Add** button and specify the following values of settings:

   - In the **Tool name** field, enter any name for the tool (for example, `VNC`).
   - In the **Executable file name** field, enter the full path to the executable file of the VNC client (for example, `C:\Program Files\TightVNC\tvnviewer.exe`).
   - In the **Working directory** field, enter the full path to the working folder of the VNC client (for example, `C:\Program Files\TightVNC\`).
   - In the **Command line** field, enter the following value: `<A>:<P>`.
   - Select the **Create tunnel for TCP port specified below** check box and enter the number of the VNC port on the VNC server (for example, if the VNC server uses screen :3, enter the VNC port number `5903`).
4. After the external VNC tool is started, a password prompt window appears. Enter the password for the VNC connection.

The opened window displays the desktop of the computer on which the Kaspersky Industrial CyberSecurity for Networks Server is installed.

Centrally monitoring systems with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console (hereinafter also referred to as "the Web Console") provides expanded capabilities for centrally monitoring the security state of information systems running Kaspersky Industrial CyberSecurity for Networks. These expanded capabilities are available when using the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in (hereinafter also referred to as "the web plug-in") in the Web Console. To use the web plug-in, it must be installed on the computer that has the Kaspersky Security Center Web Console installed.

After installing and configuring the web plug-in, you can do the following in the Web Console:

- Monitor systems controlled by Kaspersky Industrial CyberSecurity for Networks and the Kaspersky Industrial CyberSecurity for Networks Servers by using web widgets designed only for working with Kaspersky Industrial CyberSecurity for Networks.
- Search devices and events in the databases of selected Kaspersky Industrial CyberSecurity for Networks Servers using various filtering criteria.
- Map components and groups of components of Kaspersky Industrial CyberSecurity for Networks on geographic, schematic or other images to arrange objects based on their location.
- Group components of Kaspersky Industrial CyberSecurity for Networks into organizational units (hereinafter also referred to as "sites") that logically delimit the areas of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks.

When using the functions listed above, you can quickly switch from the Web Console to connect to the necessary Kaspersky Industrial CyberSecurity for Networks Servers through the web interface. If Single Sign-On technology is in use, users who were created in Kaspersky Industrial CyberSecurity for Networks do not have to enter their account credentials when connecting to a Kaspersky Industrial CyberSecurity for Networks Server. Users who have logged in to the Web Console can also complete authentication.

About the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in

The Kaspersky Industrial CyberSecurity for Networks Administration web plug-in facilitates interaction between the application and the Kaspersky Security Center Web Console.

The web plug-in is not installed in the Web Console by default. In contrast to the Management Plug-in for the Kaspersky Security Center Administration Console, which is installed on the administrator's workstation, the web plug-in must be installed on the computer that has the Kaspersky Security Center Web Console installed. The functionality of the web plug-in is available to all administrators that have access to the Web Console in a browser.

You can view the list of installed web plug-ins in the Web Console interface: **Console settings** → **Web plug-ins**.

Installing the web plug-in

You can install the web plug-in by using any of the following methods:

- Install the web plug-in from the list of available distribution packages in the Web Console.

  To install the web plug-in, select the web plug-in distribution package in the Web Console interface: **Console settings** → **Web plug-ins**. The list of available distribution packages is updated automatically after new versions of Kaspersky applications are released.

- Download the distribution package to the Web Console from an external source.

  To install the web plug-in, add the ZIP archive of the web plug-in distribution package in the Web Console interface: **Console settings** → **Web plug-ins**. The distribution package of the web plug-in can be downloaded from the Kaspersky website, for example. For a local version of the application, you also need to download a text file containing a signature.

- Download the distribution package from the list of available distribution packages, plug-ins and patches for Kaspersky Security Center.

To install the web plug-in, select the web plug-in distribution package in the Web Console interface: **Operations → Kaspersky applications → Current application versions**. The list of available distribution packages is updated automatically after new versions of Kaspersky applications are released.

Updating the web plug-in

If a new version of the web plug-in becomes available, the Web Console displays the *Updates are available for utilized plug-ins* notification. You can proceed to update the web plug-in version from this Web Console notification. You can also manually check for new web plug-in updates in the Web Console interface (**Console settings → Web plug-ins**). The previous version of the web plug-in will be automatically removed during the update.

> When the web plug-in is updated, existing components (such as the added widgets or map images) are saved. The new settings of components that implement new functions of Kaspersky Industrial CyberSecurity for Networks will have the default values.

You can update the web plug-in by using any of the following methods:

- Update the web plug-in in the list of web plug-ins in online mode.

  To update the web plug-in, select the distribution package of the Kaspersky Industrial CyberSecurity for Networks web plug-in in the Web Console interface and start the update (**Console settings → Web plug-ins**). The Web Console checks for available updates on Kaspersky servers and downloads the relevant updates.

- Update the web plug-in from a file.

  To update the web plug-in, select the ZIP-archive of the distribution package for the Kaspersky Industrial CyberSecurity for Networks web plug-in in the Web Console interface: **Console settings → Web plug-ins**. The distribution package of the web plug-in can be downloaded from the Kaspersky website, for example. For a local version of the application, you also need to download a text file containing a signature.

  You can only update the web plug-in to a more recent version. The web plug-in cannot be updated to an older version.

Scenario for Single Sign-On (SSO) technology usage preparations

When working in combination with Kaspersky Security Center, you can use Single Sign-On (SSO) technology. This enables users that already logged in to the Kaspersky Security Center Web Console to also successfully complete authentication when connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. This means that any user accounts that are allowed to work with the Kaspersky Security Center Web Console (including Active Directory® users) can connect to the Server using their own account credentials.

Single Sign-On technology is available for use with Kaspersky Industrial CyberSecurity for Networks in the compatible versions of Kaspersky Security Center:

The Single Sign-On (SSO) technology usage preparations scenario consists of the following steps:

1. **Verifying and fulfilling the required conditions for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center**

   At this step, you need to verify fulfillment of all conditions for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center. If any of the conditions is not fulfilled, ensure that they get fulfilled. For example, if the functionality for interacting with Kaspersky Security Center is not configured in Kaspersky Industrial CyberSecurity for Networks, enable and configure this functionality.

2. **Enabling and configuring the Kaspersky Security Center Web Console Identity and Access Manager (IAM) component**

   At this step, the scenario for enabling Identity and Access Manager is executed as described in the Kaspersky Security Center Help System.

   When configuring the IAM component, it is recommended to specify the DNS name of the computer as the network name of the device only if the computer is accessible by this name from the Kaspersky Industrial CyberSecurity for Networks Server computer. If it is accessible only by IP address, specify this IP address instead of the DNS name.

3. **Registering the Kaspersky Industrial CyberSecurity for Networks Server as a client for the IAM component**

   At this step, the IAM component detects Kaspersky Industrial CyberSecurity for Networks Servers that are prepared for registration as clients for this component. You need to accept the request for Server registration after it is detected. Detected and registered clients of the IAM component are displayed in a table that you can open in the Kaspersky Security Center Web Console under **Console settings** → **Integration** → **Identity and Access Manager**. To register Servers, open the table by clicking the **Settings** link in the section containing information about registered clients, select the check boxes next to the relevant Servers, and click **Approve**.

   After you have confirmed registration of the IAM component client, you need to wait for the preparation process to finish. When synchronization between the IAM component and the client is completed, the ready status will be displayed for this client. If the status has not changed, click the **Update** button.

   > The IAM component needs some time to detect clients and synchronize with them. Depending on the workload of the Kaspersky Security Center Administration Server and the Kaspersky Industrial CyberSecurity for Networks Server, it may take up to 15 minutes to complete these actions.

4. **Preparing users with access permissions for connecting to Kaspersky Industrial CyberSecurity for Networks**

   At this step, you need to grant access permissions to Kaspersky Security Center users corresponding to the Administrator and Operator roles of Kaspersky Industrial CyberSecurity for Networks. For this purpose, you can use existing user accounts or new accounts of users and groups that were created specifically for granting only these permissions.

When this scenario is fulfilled, Kaspersky Industrial CyberSecurity for Networks will have the capability to connect to the Server through the web interface using the account credentials of Kaspersky Security Center users. To do so, you can use the **Kaspersky Security Center user** button on the account credentials input page for the Kaspersky Industrial CyberSecurity for Networks web interface.

> If a fully qualified domain name (FQDN) was specified for the web server and the REST API server when configuring the connection settings using Kaspersky Security Center Web Console, then when connecting to the Kaspersky Industrial CyberSecurity for Networks Server using single sign-on technology, the user must also specify this name in the address bar of the browser.

Granting Kaspersky Security Center users the access rights corresponding to their user roles in Kaspersky Industrial CyberSecurity for Networks

To utilize Single Sign-On technology and perform specific actions in the Web Console, Kaspersky Security Center users must be granted the access permissions corresponding to their user roles in Kaspersky Industrial CyberSecurity for Networks. You can grant these permissions after the file containing the configuration of the rights-based access control model (RBAC) for Kaspersky Industrial CyberSecurity for Networks has been uploaded to the Kaspersky Security Center Administration Server.

The configuration is loaded automatically after installation of the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in. If the configuration was uploaded to the Administration Server, the file named KICS4NET_<file version number>.conf was saved in the folder %ProgramData%\KasperskyLab\adminkit\1093\dat\rbac\. If the specified folder does not contain the file named KICS4NET_<file version number>.conf, create and configure the "Download updates to the Administration Server repository" task. You can select the Kaspersky update servers as the source of updates.

After loading the RBAC configuration for Kaspersky Industrial CyberSecurity for Networks, Kaspersky Security Center will provide the capability to assign users the permissions corresponding to the Administrator and Operator roles of Kaspersky Industrial CyberSecurity for Networks.

User roles in Kaspersky Industrial CyberSecurity for Networks have the following corresponding access rights in Kaspersky Security Center from the functional scope of **Kaspersky Industrial CyberSecurity for Networks: General functions**:

- **Read** – corresponds to the Operator role.
- **Write** – corresponds to the Administrator role.

Together with these rights, users must also be assigned all rights from the functional scope of the **Kaspersky Security Center Administration Server: General functions: Basic functionality** (this functional scope includes the rights to **Read**, **Write**, **Execute** and **Perform operations on device selections**).

If access rights are assigned to users by means of Kaspersky Security Center roles, then you must add the administration group containing the computer with the Kaspersky Industrial CyberSecurity for Networks Server installed to the role scope. To do so, on the **Scope definition** page in the Role Assignment Wizard, select the **Managed devices** administration group.

Web widgets for monitoring systems and Kaspersky Industrial CyberSecurity for Networks Servers

You can use web widgets to monitor systems controlled by Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Networks Servers. The Kaspersky Security Center Web Console displays web widgets in the Dashboard (under **Monitoring and reports → Dashboard**). By default, the Dashboard does not show web widgets for Kaspersky Industrial CyberSecurity for Networks. You can add the necessary web widgets after installation of the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in.

Web widgets let you show the following information in the Dashboard:

- Statuses in KICS for Networks.
- Critical events in KICS for Networks.
- Devices with issues in KICS for Networks.
- Up-to-date events of KICS for Networks.
- KICS for Networks deployment map.
- Information about KICS for Networks Servers.

Web widgets for Kaspersky Industrial CyberSecurity for Networks are included in the **Other** category in the list of available web widgets of the Web Console.

The information displayed in web widgets is automatically updated every 1–2 minutes. If no data is received from a Server after two minutes, out-of-date data in web widgets is hidden. If necessary, you can manually update the displayed information by using the relevant options in the web widget menu.

Web widget for Statuses in KICS for Networks

The **Statuses in KICS for Networks** web widget for the Web Console displays the ratio of current statuses assigned to Kaspersky Industrial CyberSecurity for Networks Servers. Information is provided only for relevant statuses (if there are no Servers with a specific status, this status is not displayed in the web widget).

The following statuses are available for Servers in the web widget:

- *Critical*.

  This status is assigned to a Server if at least one of the following conditions is fulfilled:

  - The Server has messages about disruption of application operation.
  - The Server database has unresolved events with *Critical* severity.
  - There are devices with the *Unauthorized* status.
  - The license key expired.

- *Warning*.

  This status is assigned to a Server if none of the conditions for assigning the *Critical* status are fulfilled, but at least one of the following conditions is fulfilled:

  - The Server has messages about non-critical malfunctions.
  - The Server database has unresolved events with *Warning* severity.
  - The license key will expire in less than 14 days.

- *OK*.

  This status is assigned to a Server in all other cases (if the Server is accessible and data is being received for processing).

- *Maintenance*.

  This status is assigned to a Server if the application is currently under maintenance (for example, when importing a security policy).

If the status of a Server cannot be determined, the *Unknown* status is displayed for this Server.

By default, the web widget displays status information for all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the web widget. If necessary, you can use the web widget settings menu to select the Servers whose data should be displayed in the web widget.

Web widget for Critical events in KICS for Networks

The **Critical events in KICS for Networks** web widget for the Web Console displays the ratio of unresolved events with *High* severity (corresponding to the *Critical* severity level) on Kaspersky Industrial CyberSecurity for Networks Servers. For each Server whose database contains unresolved events with *High* severity (corresponding to the *Critical* severity level), the number of these events is displayed.

> The different coloring of data presented in the web widget does not have any relation to the severity of events. Colors on the web widget chart are used only to visually distinguish events of different Servers.

By default, the web widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the web widget. If necessary, you can use the web widget settings menu to select the Servers whose data should be displayed in the web widget.

Web widget for Devices with issues in KICS for Networks

The **Devices with issues in KICS for Networks** web widget for the Web Console displays information about devices that were detected by Kaspersky Industrial CyberSecurity for Networks applications and have issues. A device requires attention (designated as "with issues") in any of the following cases:

- The security state of the device differs from *OK*.
- The device has the *Unauthorized* status.

If there are devices with issues, the web widget contains the following information:

- Number of devices with issues (in each device category). This data is displayed in the upper part of the web widget under the icons of device categories. The number of displayed categories depends on the free space in the widget. If there are more categories to display, you can open a window containing all categories by clicking the **Show all** icon.
- List of categories of devices with issues. This data is displayed in the middle part of the widget. The following information is displayed for each category in the list:
  - Line containing the category icon and comment. The end of the line provides a link containing the number of devices with issues.
  - Line containing the graphical elements representing the devices. This line is displayed if there is sufficient free space in the widget. If there are more devices with issues than the number of graphical elements displayed in the line, the number of hidden devices is displayed on the right in the format `+<number of devices>`.

By default, the web widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the web widget. If necessary, you can use the web widget settings menu to select the Servers whose data should be displayed in the web widget.

Graphical elements of devices

Graphical elements representing devices contain the following information:

- Device name.
- Device status. This is displayed as an icon if the device has the *Unauthorized* status.

- Device security state. This is displayed as a colored line on the left border of the graphical element. The color of the line corresponds to the *OK*, *Warning* or *Critical* states.

The graphical elements are displayed in the following order:

1. Devices assigned the *Unauthorized* status.
2. Devices with the *Critical* security state.
3. Devices with the *Warning* security state.

Navigating from the web widget

You can use elements of the web widget interface to display detailed information about devices. To do so, you can utilize the following options:

- **Display information about the selected device in the devices table on the Server web interface page**

  In the **Devices with issues in KICS for Networks** web widget, click the graphical element that represents the relevant device.

  The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during initial configuration of the application after installation.

  If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

  On the Server web interface page, the **Assets** section automatically opens to show the devices table. The table will be filtered based on the device ID.

- **Display information about devices of the selected category in the search results table in the Web Console**

To display information about all devices of the selected category:

In the upper part of the **Devices with issues in KICS for Networks** web widget, click the icon of the relevant category.

The **KICS for Networks** → **Search** section of the Web Console opens to display a table of device search results. The table will be filtered based on the following criteria:

- Selected category of devices
- All Servers whose data is taken into account in the web widget

To display information about all devices with issues that belong to a specific category:

In the list of categories containing devices with issues, click the link containing the number of devices of the relevant category.

The **KICS for Networks** → **Search** section of the Web Console opens to display a table of device search results. The table will be filtered based on the following criteria:

- Selected category of devices
- All Servers whose data is taken into account in the web widget
- Indicator of devices with issues

- Display information about all devices in the search results table in the Web Console

Click the **Show all devices** link in the **Devices with issues in KICS for Networks** web widget.

The **KICS for Networks** → **Search** section of the Web Console opens to display a table of device search results. The table will be filtered for all Servers whose data is taken into account in the web widget.

Web widget for Up-to-date events of KICS for Networks

The **Up-to-date events of KICS for Networks** web widget for the Web Console displays general information about Kaspersky Industrial CyberSecurity for Networks events that have the most recent values for the date and time of last occurrence.

The web widget contains the following information:

- Histogram of events for the selected period. This data is displayed in the upper part of the web widget. The histogram shows the distribution of events by severity levels.
- List of registered events. This data is displayed in the middle part of the web widget. Events are sorted by date and time of last occurrence.

By default, the web widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the web widget. If necessary, you can use the web widget settings menu to select the Servers whose data should be displayed in the web widget.

Histogram of events

On the histogram showing the distribution of events, the bars correspond to the total number of events for each time interval. Within bars, the severity of events is distinguished by color. The following colors correspond to severity levels:

- Blue – events with *Low* severity (corresponding to the *Informational* severity level).
- Yellow – events with *Medium* severity (corresponding to the *Warning* severity level).
- Red – events with *High* severity (corresponding to the *Critical* severity level).

When you move the mouse pointer over a bar of the histogram, a pop-up window showing the number of events by severity levels is displayed.

The duration of time intervals depends on the selected display period. To build the relevant histogram, you can select one of the following periods from the web widget menu:

- 1 hour. This period is divided into one-minute intervals.
- 12 hours, 24 hours. These periods are divided into one-hour intervals.
- 7 days. This period is divided into 12-hour intervals.

List of events

The number of displayed elements in the list of events is limited by the size of the web widget.

The following information is provided for each event:

- Event title
- Severity level
- Name of the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server

Navigating from the web widget

You can use elements of the web widget interface to display detailed information about events. To do so, you can utilize the following options:

- **Display information about the selected event in the events table on the Server web interface page**

Click the relevant event in the **Up-to-date events of KICS for Networks** web widget.

The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during initial configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

On the Server web interface page, the **Events** section automatically opens to show the events table. The table will be filtered based on the ID of the selected event. The period ranging from the date and time of registration of the event to the current moment (without indicating an end boundary for the period) will also be defined for the filter.

- **Display information about all events for the selected period in the search results table in the Web Console**

Click the **Show all events** link in the **Up-to-date events of KICS for Networks** web widget.

The **KICS for Networks** → **Search** section of the Web Console opens to display a table of event search results. The table will be filtered based on the following criteria:

- Currently selected period for building a histogram in the web widget
- All Servers whose data is taken into account in the web widget

Web widget for KICS for Networks deployment map

The **KICS for Networks deployment map** web widget for the Web Console displays a map depicting the geographic distribution of sites in which Kaspersky Industrial CyberSecurity for Networks components are grouped. The web widget uses a smaller copy of the main map that is available in the **KICS for Networks** → **Map** section of the Web Console.

Sites on the map are designated by icons whose color depends on the statuses of the sites. The following statuses are available for sites:

- *Critical*.

  This status is assigned to a site if it contains at least one Server with the *Critical* status.

- *Warning*.

  This status is assigned to a site if it contains at least one Server with the *Warning* status and does not contain Servers with the *Critical* or *Unknown* status.

- *OK*.

  This status is assigned to a site if it contains at least one Server with the *OK* status and does not contain Servers with the *Critical*, *Warning*, *Unknown* or *Maintenance* status.

- *Maintenance*.

  This status is assigned to a site if it contains at least one Server with the *Maintenance* status and does not contain Servers with the *Critical*, *Warning* or *Unknown* status.

- *Muted*.

  This status is assigned to a site if it contains only Servers with the *Muted* status.

- *Unknown*.

  This status is assigned to a site if it contains at least one Server with the *Unknown* status and does not contain Servers with the *Critical* status.

- *No Servers*.

  This status is assigned to a site if it does not contain any Servers.

You can proceed to the main map in the **KICS for Networks** → **Map** section of the Web Console by clicking any part of the map except the icons of sites.

You can proceed to a site map by clicking the icon of this site in the web widget.

Web widget for Information about KICS for Networks Servers

The **Information about KICS for Networks Servers** web widget for the Web Console displays general information about the current state of Kaspersky Industrial CyberSecurity for Networks Servers.

The following information is provided for each Server:

- **Server name** – name used to represent the Server in Kaspersky Security Center (device name in the administration group).

- **Functions** – information about the current state of protection functions in Kaspersky Industrial CyberSecurity for Networks. The following values are possible:

  - **All ON** – all technologies and methods designed for continual use are enabled, and all created monitoring points are enabled.

  - **Not all ON** – some protection functions are disabled or are enabled in learning mode, or not all monitoring points are enabled.

- **Status** – current status of the Server.

- **Application message** – last application message or additional status information.

By default, the web widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If necessary, you can use the web widget settings menu to select the Servers whose data should be displayed in the web widget.

You can click the link containing a Server name to open the web interface page of the selected Kaspersky Industrial CyberSecurity for Networks Server. The name of the opened browser tab will be the Server name that was defined during initial configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

Searching devices and events in the databases of Kaspersky Industrial CyberSecurity for Networks Servers

In the Kaspersky Security Center Web Console, you can create requests to receive specific selections of devices and events by using the Kaspersky Industrial CyberSecurity for Networks web plug-in. Based on these requests, a search is performed directly in the databases of Kaspersky Industrial CyberSecurity for Networks Servers. This is the main distinction between the web plug-in capabilities and the search functionality provided by the standard tools for receiving selections of devices and events in the Web Console (for example, under **Devices** → **Device selections** and **Monitoring and reports** → **Event selections**). When using the standard tools in the Web Console, the search for devices and events is performed in the Administration Server database.

The **KICS for Networks** → **Search** section of the Web Console is used to configure the settings of search requests sent to Kaspersky Industrial CyberSecurity for Networks Servers and to display the search results. Search requests for devices must be formulated separately from search requests for events.

Kaspersky Industrial CyberSecurity for Networks Servers process the search requests and provide information for those requests with the following limitations:

- The number of returned items that match the search request (devices or events) from each Server cannot be more than 200.
- They provide only the information that can actually be searched. For example, device search results will contain the MAC- and IP addresses of devices but will not contain information about the device models and manufacturers.

In any case, when you need to obtain complete information about any found devices or events, you can go to the web interface page of the Server by using the interface elements under **KICS for Networks** → **Search**. The Server web interface page automatically opens the corresponding section (**Assets** or **Events**), which will be filtered based on the criteria of the search request or the obtained results.

Configuring the device search settings

You can manually configure the device search settings or use automatically applied filtering criteria when navigating directly from the **Devices with issues in KICS for Networks** web widget.

To manually configure these settings, you need to open the **Devices** tab in the search request details area.

*To open the **Devices** tab in the search request details area:*

1. Go to the **KICS for Networks** → **Search** section of the Web Console.
2. Do one of the following:
   - If a search request was not created during the current session and this section is not displaying a search results table, click the **Find events or devices** button.
   - If a search request was created in the current session and this section is displaying a search results table, click the **Search** button in the toolbar.

     The **Search** button displays the number of filtering criteria (defined settings) of the current search request.
3. In the search request details area, go to the **Devices** tab.

After configuring the settings, you can start searching for devices in the databases of Servers by using the **Find** button.

You can configure the following settings in a device search request:

- **Name** – name used to represent the device in the devices table of the Kaspersky Industrial CyberSecurity for Networks Server. The complete name must be specified.
- **Servers** – names used to represent the Servers in Kaspersky Security Center (device names in administration groups).
- **Addresses** – MAC- and/or IP addresses of devices. Complete addresses must be provided.
- **Statuses** – device statuses that determine whether activity of the devices is allowed in the industrial network.
- **Security states** – device security states that are determined by the severity of registered events linked to the device and current vulnerabilities.
- **Categories** – names of the categories that determine the functional purpose of devices.
- **With issues** – indicates whether a device has issues requiring attention.

You can clear the defined settings in a search request by clicking the **Reset filters** button.

Configuring the event search settings

You can manually configure the event search settings or use automatically applied filtering criteria when navigating directly from the **Up-to-date events of KICS for Networks** web widget.

To manually configure these settings, you need to open the **Events** tab in the search request details area.

*To open the **Events** tab in the search request details area:*

1. Go to the **KICS for Networks** → **Search** section of the Web Console.
2. Do one of the following:
   - If a search request was not created during the current session and this section is not displaying a search results table, click the **Find events or devices** button.
   - If a search request was created in the current session and this section is displaying a search results table, click the **Search** button in the toolbar.

     The **Search** button displays the number of filtering criteria (defined settings) of the current search request.
3. In the search request details area, go to the **Events** tab.

After configuring the settings, you can start searching for events in the databases of Servers by using the **Find** button.

You can configure the following settings in an event search request:

- **Title** – title defined for the event type in Kaspersky Industrial CyberSecurity for Networks. The complete title must be specified.

- **Servers** – names used to represent the Servers in Kaspersky Security Center (device names in administration groups).
- **Last seen** – period for filtering events by date and time of last appearance.
- **Source** – address information (MAC/IP addresses or port numbers) of the senders of network packets.
- **Destination** – address information (MAC/IP addresses or port numbers) of the recipients of network packets.
- **Technologies** – icons and names of technologies that were used to register the events.
- **Severity** – icons and names of the event severity levels.

You can clear the defined settings in a search request by clicking the **Reset filters** button.

Viewing the search results table

The search results table for devices or events is displayed in the **KICS for Networks** → **Search** section of the Web Console. The table shows only the data that can be used to perform a device search or event search. Any found items are grouped based on their respective Servers.

When viewing the table, you can utilize the following functions:

- Filtering search results ?

  To filter the search results table, you can utilize the following interface elements in the toolbar:

  - **Security states**

    This filter is available in the results table for device searches. You can use the filter buttons to hide some of the found devices depending on their security states.

  - **Severity**

    This filter is available in the results table for event searches. You can use the filter buttons to hide some of the found events depending on their severity levels.

  - **Technologies**

    This filter is available in the results table for event searches. You can use the filter buttons to hide some of the found events depending on the technologies that were used to register them.

  - **Servers**

    This drop-down list lets you select specific Servers for displaying search results.

- Updating search results ?

  Information about devices or events could be changed on the Servers while you are viewing the search results table. The **Last update** field displays the date and time when the results were last loaded.

  You can repeat a search request to update the results by clicking the **Update** button in the toolbar.

- Displaying information on Server web interface pages ?

Do one of the following:

- To receive detailed information about one of the found items, open the web interface page of the corresponding Server by clicking the link containing the device name or the event title.
- To receive information about all the found items that meet the search request criteria, open the web interface page of the corresponding Server by clicking the **Go to Server** link.

The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during initial configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

On the Server web interface page, the relevant section automatically opens to show the devices table or events table. The table will be filtered based on the corresponding criteria.

Mapping components of Kaspersky Industrial CyberSecurity for Networks

The web plug-in lets you create maps depicting the deployment of Servers and sensors of Kaspersky Industrial CyberSecurity for Networks in the Kaspersky Security Center Web Console. You can use maps to arrange these items based on their geographic location and to monitor their state in a view that is convenient for you.

The **KICS for Networks** → **Map** section of the Web Console is designed for working with maps. This section displays the following maps (only one map can be selected at one time):

- Main map. This map depicts the various sites (organizational units used to group components of Kaspersky Industrial CyberSecurity for Networks). Servers and sensors are not displayed at this level.
- Site maps. Each site map contains the application components (Servers and sensors) that are included in this particular site.

On maps, sites and application components are represented by icons containing the names of these objects. Long names are abbreviated to their first characters.

Background images can be displayed in various scales. To manage the display scale, you can use the toolbar located in the upper part of the **KICS for Networks** → **Map** section of the Web Console.

After navigating from the main map to a site map, you can return to the main map by using the arrow button.

Only Kaspersky Security Center users who have been granted the access permissions for the Administrator role in Kaspersky Industrial CyberSecurity for Networks can create maps and arrange objects on those maps. When configuration is complete, users with access permissions for the Operator role can track the state of objects by using the maps in the Web Console under **KICS for Networks** → **Map** and in the **KICS for Networks deployment map** web widget.

Generating a list of sites for the main map

When working with the main map in the **KICS for Networks** → **Map** section of the Web Console, you can generate a list of sites that will be used to delimit the zones of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks. You can add relevant Servers and perform operations with these Servers and their sensors within sites.

The maximum number of sites is 100.

A list of sites can be generated only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

You can use the following functions to generate a list of sites:

- **Adding a site**

  1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
  2. Select **KICS for Networks** → **Map**.
  3. Click the **Show list of sites** button.

     The **Sites** window will appear in the right part of the section.
  4. Click **Add**.

     A window for entering the site name appears.
  5. Enter the site name.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

     The site name must meet the following requirements:

     - Must begin and end with any permitted character except a space.
     - Must contain 255 characters or less.
     - Must not match the name of another site.

     The **Sites** window will show a line containing the name of the new site.
  6. If a line containing the site name has not appeared in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking the **All statuses** button or enable the display of sites without Servers by clicking the **No Servers** button.
  7. Add the site to the main map. To do so, move your cursor over the line containing the site name and click the 📍 button.
  8. Move the site icon to the necessary place on the map.

- **Renaming a site**

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant site.

5. Move your cursor over the line containing the site name and click the ✎ button.

   A window for entering the site name appears.

6. Enter the site name.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   The site name must meet the following requirements:

   - Must begin and end with any permitted character except a space.

   - Must contain 255 characters or less.

   - Must not match the name of another site.

- Deleting a site

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant site.

5. Move your cursor over the line containing the site name and click the × button.

6. In the confirmation prompt window, click **OK**.

Changing the background image of a map

After a map is created, the map uses the default background image. You can change the background image to any image you want. For example, you can use the image of a geographic map of any territory for the main map, and you can upload equipment deployment schematics of workshops and work areas for site maps.

For a map background, you can use images uploaded from JPG or PNG files. The maximum size of an uploaded file is 50 MB. The minimum size of an image in an uploaded file is 600x600 pixels. After a new image is uploaded, the old image is deleted and the positions of all objects on the map are cleared.

The background image on maps can be changed only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

To change the background image for the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Replace image** button.

   You will see a window prompting you to drag the image file or select a file.

4. Use any convenient method to upload the file.

To change the background image for a site map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click the **Replace image** button.

   You will see a window prompting you to drag the image file or select a file.

6. Use any convenient method to upload the file.

Generating lists of Servers within sites

On the maps of created sites under **KICS for Networks** → **Map** in the Web Console, you need to generate lists of Servers residing at these sites based on the delimited zones of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks. Any Servers residing at sites also include the sensors that are associated with these Servers.

Each Kaspersky Industrial CyberSecurity for Networks Server can be included in only one site. Any Server that was not added to a site will remain on the **Outside of sites** list until it is included in a site.

Lists of Servers at sites can be generated only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

You can use the following functions to generate a list of Servers:

- Adding a Server to a site

  1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
  2. Select **KICS for Networks** → **Map**.
  3. Click the **Show list of sites** button.

     The **Sites** window will appear in the right part of the section.
  4. Click the line containing the name of the relevant site.

     The site map opens.
  5. Click the **Show list of Servers** button.

     A window containing the site name will appear in the right part of the section.
  6. Select the **Outside of sites** tab.
  7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant Server.
  8. Move your cursor over the line containing the Server name and click the + button.

     The Server line will no longer be displayed on the **Outside of sites** tab.
  9. Select the **In site** tab.
  10. If a line containing an added Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the Server.
  11. Add the Server to the site map. To do so, move your cursor over the line containing the Server name and click the 📍 button.

      After this operation is performed, the brightness of the icon in the button changes.
  12. If there are sensors associated with the Server and you want to enable the display of these sensors, expand the **Sensors** list and add them by using the 📍 buttons.
  13. Move the icons of objects to their proper positions on the map.

- Removing a Server from a site

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click the **Show list of Servers** button.

   A window containing the site name will appear in the right part of the section.

6. Select the **In site** tab.

7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant Server.

8. Move your cursor over the line containing the Server name and click the × button.

   The Server will appear on the **Outside of sites** tab.

Managing the arrangement of objects on maps

In the **KICS for Networks** → **Map** section of the Web Console, sites and components of Kaspersky Industrial CyberSecurity for Networks are represented by icons on maps.

The arrangement of objects on maps can be managed only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

You can move the icons of objects to their necessary locations on maps. However, all icons on a map must be displayed separately without completely overlaying each other.

If necessary, you can disable the display of an irrelevant object on a map. After being disabled from the display, an object is not deleted from the list of map objects. You can re-enable the display of this object at a later time.

To enable or disable the display of a site on the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant site.

5. Move your cursor over the line containing the site name and click the 📍 button.

   After this operation is performed, the brightness of the icon in the button changes.

To enable or disable the display of a Server or sensor on the site map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click the **Show list of Servers** button.

   A window containing the site name will appear in the right part of the section.

6. Select the **In site** tab.

7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking the **All statuses** button or click the button containing the name of the status that was assigned to the relevant Server.

8. If there are sensors associated with the Server and you want to enable or disable the display of these sensors, expand the **Sensors** list in the line containing the name of the relevant Server.

9. Move your cursor over the line containing the name of the relevant Server or sensor and click the 📍 button.

   When you disable the display of a Server, this simultaneously enables the display of all sensors associated with this Server.

   After this operation is performed, the brightness of the icon in the button changes.

Muting a Server in the Web Console

If the Kaspersky Security Center Web Console is receiving data from multiple Kaspersky Industrial CyberSecurity for Networks Servers and data from a specific Server does not require monitoring for a certain period of time (for example, during preventative maintenance and adjustment operations in the ICS), you can exclude this Server from monitoring ("mute" the Server). After you mute a Server, the Web Console will stop receiving data from this Server and will assign the *Muted* status to it. However, the Kaspersky Security Center Administration Server will continue receiving and saving data from this Server (including events).

The Server will remain muted until you re-enable monitoring for this Server ("unmute" the Server).

Servers can be muted and unmuted only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

To mute or unmute a Server:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.
4. Click the line containing the name of the relevant site.

   The site map opens.
5. Click the **Show list of Servers** button.

   A window containing the site name will appear in the right part of the section.
6. Click the line containing the name of the relevant Server.

   A window containing detailed information about the Server will appear in the right part of the section.
7. If you want to mute the Server, click the **Mute** button. If the Server was already muted and you want to unmute it, click the **Unmute** button.
8. In the confirmation prompt window, click **OK**.

Viewing information about Servers on maps

The statuses of Kaspersky Industrial CyberSecurity for Networks Servers affect the colors of the displayed icons for Servers and the icons of sites on maps in the **KICS for Networks** → **Map** section of the Web Console. If icons of sensors are displayed on a site map, the colors of these icons depend on the current state of the nodes containing the sensors. This lets you keep track of the statuses of Kaspersky Industrial CyberSecurity for Networks components based on the colors of icons representing the objects on maps.

If necessary, you can view detailed information about each Server. The detailed information window provides the main data on the current state of the Server, information about installed updates of application modules and databases, data on hardware resource usage, and license key details.

To view detailed information about a Server:

1. Select **KICS for Networks** → **Map**.
2. Click the **Show list of sites** button.

   The **Sites** window will appear in the right part of the section.
3. Click the line containing the name of the relevant site.

   The site map opens.
4. Click the **Show list of Servers** button.

   A window containing the site name will appear in the right part of the section.
5. Click the line containing the name of the relevant Server.

   A window containing detailed information about the Server will appear in the right part of the section.
6. If you want to go to the web interface page of the Server, click the **Go to Server** button.

The browser will open a tab showing the Server name that was defined during initial configuration of the application after installation.

Troubleshooting

This section contains a description of possible problems in the operation of Kaspersky Industrial CyberSecurity for Networks and methods for resolving them.

The application cannot be installed due to an unavailable repository for DNF

Problem

When installing the application on a computer running the CentOS operating system, you see a message stating that the repository for the DNF software package manager is not available. Application installation is interrupted.

Solution

The application cannot be installed if the repositories containing the installation packages for the operating system are unavailable (or incorrectly configured) in the DNF software package manager. To install the application, unavailable repositories must be disabled.

To disable unavailable repositories and install the application:

1. Load the list of all connected repositories of the DNF package manager. To do so, open the operating system console and type the following command in the command line:

   ```
   dnf repolist
   ```

2. Find the unavailable repositories on the list and disable them. To disable a repository, type the following command in the command line:

   ```
   sudo dnf config-manager --set-disabled <repository name>
   ```

3. Reinstall the application with the same installation settings.

An application component cannot be installed on a selected node

Problem

During centralized installation of application components, there is a message stating that a node is unavailable for component installation due to failure to connect over the SSH protocol. The component is not installed on this node.

Solution

Centralized installation of an application component is impossible if the address information or network name of the computer was changed after configuring access over the SSH protocol on the node where the component will be installed. To centrally install the application component, you must restore access to the remote computer over the SSH protocol.

To restore access over the SSH protocol and install the application component:

1. On the computer from which the centralized installation of application components is performed, update the key used for connecting to the node over the SSH protocol. To do so, sign in to the system using the account credentials of the user account used to install the application, and enter the following command in the operating system console:

   ```
   sudo ssh-keygen -R <node IP address>
   ```

2. Reinstall the application with the same installation settings. During reinstallation, make sure that there is no message stating that the node is unavailable for component installation.

Application problems detected

Problem

When connected to the Server through the web interface, the upper part of the application web interface menu displays a red icon next to the 🔔 button.

Solution

This state of Kaspersky Industrial CyberSecurity for Networks signifies that one of the application processes is malfunctioning.

To restore operation of the application:

1. Wait 20-30 seconds.

   The application may resume normal operation automatically. If the application resumes normal operation, the red icon will no longer be displayed.

2. If the malfunction persists, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

New application message

Problem

A new application message appears in the **Settings** → **Application messages** section.

> Messages requiring attention are indicated by a red or yellow icon next to the 🔔 button in the web interface menu. If the icon is displayed, this means that there is a message regarding disruption of application operation or about a non-critical malfunction, and this problem has not been resolved. To view information, you can go to the **Settings** → **Application messages** section by using the 🔔 button when a red or yellow icon is displayed next to this button.

Solution

An application message means that some event occurred in the application.

Read the concise information in the message under **Settings** → **Application messages**. Based on this information, you can make a decision on the necessary actions.

The next steps depend on the message status. The following statuses are available for messages:

- *Normal operation* – in most cases, the message does not require a response. However, there may be situations requiring additional clarification of the circumstances. For example, this may be necessary when you receive a message about the successful application of a security policy when you do not know why this action was taken.
- *Unknown*, *Malfunction* – if the message just recently appeared, wait 20–30 seconds and check the current state of the application.
- *Moderate malfunction*, *Critical malfunction* or *Fatal malfunction* – the application is malfunctioning. If the issue could not be resolved, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

Not enough free space on hard drive

Problem

There is not enough free space on the computer hard drive where the Application Server or sensor is installed.

Solution

The computer must meet the hardware and software requirements to ensure proper functioning of application components.

For the application to function correctly:

1. On the hard drive of the computer, free up sufficient space to satisfy the minimum free disk space requirements.
2. Restart the services supporting operation of application components.

An error occurs when enabling a monitoring point

Problem

After the monitoring point switches to the *Enabled* mode, the *Error* status is displayed. As a result, the node associated with this monitoring point is displayed in the *Operation disrupted* status. The list of notifications about application operating issues also shows a message regarding disrupted operation due to detected issues at the monitoring point.

Solution

The *Error* status of the monitoring point may be associated with an unsupported operational state of a network interface. For successful completion of a scan when a monitoring point is enabled, the network interface must have the *UP* operational state. If the network interface is in a different operational state (for example, *UNKNOWN*), the application assigns the *Error* status to the monitoring point because of possible problems when receiving or processing network packets.

You can use the `ip link` command to check the current operational state of a network interface on a node computer. Information about the current operational state is displayed in the string containing the name of the interface in the following format: `state <state>`. The most likely operational states on a problematic network interface are as follows:

- *DOWN*. In this case, you can switch the interface to the *UP* operational state by using the following command:

  ```
  sudo ip link set <interface name> up
  ```

- *UNKNOWN*. This operational state may be due to an incorrectly added interface. For example, network interfaces that were added by default on a VMware™ virtual machine may operate in the *UNKNOWN* state. In this case, it is recommended to re-add (create) a network interface with the correct settings by using the corresponding resources for managing network interfaces.

When the network interface switches to the *UP* operational state, check the status of the monitoring point added to this network interface. If the monitoring point is still displayed as having the *Error* status, disable and then re-enable this monitoring point.

No traffic at monitoring point

Problem

The application has registered an event whose description contains the following text: `No traffic at monitoring point`. The event description includes the duration of the absence of traffic, the name of the monitoring point, and the network interface that is not receiving traffic.

Solution

For traffic to arrive at the monitoring point, the following conditions must be met:

- The monitoring point is enabled and its current status is *OK*.
- On the network interface of the monitoring point, the network cable is connected to the Ethernet port.
- The rate of incoming traffic is more than 0 bps at the network interface of the monitoring point.

You can view information about monitoring points and network interfaces when connected to the Server through the web interface in the **Settings** → **Deployment** section.

If the displayed rate of incoming traffic is 0 bps at the network interface of the monitoring point, verify that the following conditions are met:

- The network interface of the monitoring point is correctly configured in the operating system.
- When the network interface is connected to the industrial network switch, transmission of mirrored traffic through the connection port (SPAN) must be correctly configured on the network switch.

Traffic is not being loaded for events or incidents

Problem

Cannot load traffic for the selected events and/or incidents. The events table either does not display the tools for loading traffic (for example, the **Download traffic** button is missing from the details area when one event is selected), or displays the message `No traffic for the selected events` (when attempting to load traffic).

Solution

Saved traffic for the selected events and/or incidents may be missing for one of the following reasons:

- The traffic was not saved.
- The traffic was deleted from the database.
- Traffic dump files were deleted.

The application saves traffic during event registration if the saving of traffic is enabled for the specific type of event. By default, saving of traffic is disabled for all event types. You can enable and configure the saving of traffic for relevant event types.

The application deletes saved traffic for registered events when one of the traffic storage limits is reached (for example, upon reaching the maximum volume of saved traffic in the database). Traffic packets that were saved before other packets are deleted from the database. If saved traffic is deleted too quickly and you do not have time to load it for relevant events, you can increase the maximum values of traffic storage settings.

When the limit is reached for stored traffic dump files, the application deletes temporary traffic dump files that were saved earlier than other files. If traffic dump files are being deleted faster than you are able to load traffic from these files, you can increase the maximum values of the traffic dump file storage settings or connect external storage on nodes.

Preventative maintenance and adjustment operations on the ICS

Problem

Preventative maintenance and adjustment operations on the ICS can create a large number of important and critical events in Kaspersky Industrial CyberSecurity for Networks.

Solution

While conducting preventive maintenance and adjustment operations, you can select one of the following options for resolving this problem:

- Leave all monitoring points and all technologies enabled on the Server and on application sensors. In this case, when viewing information about events and interactions of devices, take into account the time and list of preventive maintenance and adjustment operations to be conducted.
- Disable monitoring points or disable the use of technologies on monitoring points that receive traffic from industrial network segments where preventative maintenance and adjustment operations will be conducted. For example, if the work will be conducted in only one shop, you can disable the monitoring point that receives traffic from this shop and leave all other monitoring points enabled.
- Disable all monitoring points on all nodes that have application components installed. You can select this option if preventative maintenance and adjustment operations are to be conducted throughout the entire industrial network.

If you have disabled monitoring points or technologies, to resume control of the protected ICS you need to re-enable the monitoring points or technologies immediately after completion of preventative maintenance and adjustment operations.

Bear in mind that intruders may attempt to gain unauthorized access to the network during maintenance and commissioning operations on the ICS. Follow the security regulations and procedures in place at your enterprise when deciding to disable monitoring points or technologies.

If the composition or settings of the industrial network equipment were changed while conducting preventative maintenance and adjustment operations (for example, MAC addresses and IP addresses were changed), make the appropriate changes for Process Control, Interaction Control, and Asset Management. For example, you can configure the technology learning mode for the corresponding monitoring points.

Unexpected system restart

Problem

Unexpected restart of a computer hosting a component of Kaspersky Industrial CyberSecurity for Networks.

Solution

Wait for the computer reboot to finish. After the computer has restarted, the following states of Kaspersky Industrial CyberSecurity for Networks are possible:

- Kaspersky Industrial CyberSecurity for Networks has resumed normal operation.

  The application is operating normally.
- Normal operation of Kaspersky Industrial CyberSecurity for Networks has not resumed.

  The application informs of detected operating issues.

If the malfunction persists, restart the services that support operation of application components. If the problem is not resolved after the restart, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

Connector and remote connection functionality is unavailable after changing or adding the Server IP address

Problem

If the IP address for connecting via the web server has been changed or added on the Server machine, the connectors cannot connect to the Server at the new IP address due to certificate validation errors. Device scanning with application sensors is unavailable when using the **Remote connection** polling method.

Solution

To use a new Server IP address, you need to replace/reissue the main Server certificate used for securing connections with connectors and application component services.

> Main Server certificate replacement is part of the procedure of renewing certificates for connections between Kaspersky Industrial CyberSecurity for Networks nodes. As a result, when the main Server certificate is replaced, the old application sensor certificates are invalidated, which terminates any sensor-Server connections. To resume connections as part of the certificate renewal procedure, you will need to re-add and reconnect all sensors. You will also need to update the certificates used for connecting connectors.

To replace the main Server certificate and ensure that it can be used by connectors and application component services:

1. On the Server computer, go to the /opt/kaspersky/kics4net/sbin/ folder and enter the command to launch the script for local certificate update:

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. After the script finishes, return all sensors to the initial state using the kics4net-reset-to-defaults.sh script that reverts the node to the initial state. The script is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

3. Add and connect sensors again.

4. Update the certificates used for connecting connectors.

   You can update certificates for connecting unmanageable connectors (or connectors configured to ignore the functions of a manageable connector) when creating new communication data packages for connectors. To update the certificates of manageable connectors, you must remove these connectors and then add them again.

Updates from the Kaspersky Security Center Administration Server are not received

Problem

When starting the database and application module update process with the selected update source, the **Kaspersky Security Center Administration Server** displays the message: `Update installation failed due to an error that interrupted the process.`

Solution

Downloading updates from the Kaspersky Security Center Administration Server is possible if the conditions for communication between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center are met. If any of the conditions is not fulfilled, ensure that they get fulfilled. For example, if the current version of the Kaspersky Industrial CyberSecurity for Networks administration plug-in for Kaspersky Security Center is not installed, install the plug-in.

In certain cases, update installation errors may be associated with inability to download updates from the Kaspersky Security Center repository. If updates for Kaspersky Industrial CyberSecurity for Networks have been uploaded to the update repository but are not available for download, you can perform the steps to clear the repository as described in the Kaspersky Security Center Knowledge Base ↗ .

After the Kaspersky Security Center Administration Server is reinstalled, Network Agent cannot be synchronized

Problem

If the settings from a backup copy were not restored after reinstalling the Kaspersky Security Center Administration Server, the Kaspersky Security Center Administration Console does not show the computer on which Kaspersky Industrial CyberSecurity for Networks is installed.

Solution

To restore synchronization of Network Agent, you can restore the settings of the Kaspersky Security Center Administration Server by using the klbackup utility. The klbackup tool is included in the Kaspersky Security Center distribution package. For detailed information on backup copying and restoring the settings of the Kaspersky Security Center Administration Server, please refer to the Kaspersky Security Center Help system.

If for some reason it is not possible to restore the settings of the Kaspersky Security Center Administration Server using the klbackup utility, you can restore synchronization of Network Agent by using the klmover utility that is included in Network Agent.

To use the klmover utility to restore synchronization of Network Agent:

1. On the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server, open the operating system console and go to the folder /opt/kaspersky/klnagent64/bin/.
2. Enter the following command in the command line:

   ```
   sudo ./klmover -address <IP address or computer name>
   ```

   where `<IP address or computer name>` is the IP address or name of the computer with Kaspersky Security Center.
3. After the klmover utility finishes, check the connection of Network Agent to the Kaspersky Security Center Administration Server. To do so, type the following command in the command line:

   ```
   sudo ./klnagchk
   ```

The screen will display information about the connection to the Administration Server.

After Network Agent synchronization is successfully restored, the Kaspersky Security Center Administration Console will show the computer on which Kaspersky Industrial CyberSecurity for Networks is installed.

Unable to connect to the Server through the web interface

Problem

When attempting to connect to the Server, the Kaspersky Industrial CyberSecurity for Networks web interface page does not load.

Solution

Possible situations:

- There is no network access to the Kaspersky Industrial CyberSecurity for Networks Server computer that has the web server installed. Check the connection with the computer based on the specified Server name (for example, using the `ping` command).
- Incorrect data has been entered into the browser address bar. Enter the IP address or computer name of the Server that was specified for the web server under **Settings** → **Connection Servers**. If the default port 443 is set, you do not have to specify the port number. If a different port number is specified, enter the full address in the `https://<Server name>:<port>` format in the address bar.
- JavaScript is disabled in the browser. A message about this is displayed on the connection failure warning page. In the browser settings, enable the execution of JavaScript and refresh the page.
- Access to the Server computer is blocked by the firewall. Properly configure the firewall that is being used.

When connecting to the Server, the browser displays a certificate warning

Problem

When attempting to connect to a computer that has a Kaspersky Industrial CyberSecurity for Networks component installed, the browser displays a warning that the security certificate or the connection being established is not trusted. The contents of the warning depend on the specific browser being used.

Solution

The warning means that a self-signed certificate is being used on the web server. To obtain and use a trusted certificate, you need to contact the administrator.

You can temporarily use a self-signed certificate to connect to the Server (for example, when testing the operation of Kaspersky Industrial CyberSecurity for Networks). When using a self-signed certificate, in the browser warning window select the option that lets you continue connecting. After connecting to the Server, the browser window will display a warning message about the certificate. The text of the message depends on the specific browser being used.

To continually use a certificate, you can add a trusted certificate for the web server under **Settings → Connection Servers**.

Contacting Technical Support

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

How to get technical support

If you cannot find a solution to your issue in the application documentation or in other sources of information about Kaspersky Industrial CyberSecurity for Networks, we recommend that you contact Technical Support. Our Technical Support experts will answer your questions about installing and using Kaspersky Industrial CyberSecurity for Networks.

> Kaspersky provides support for Kaspersky Industrial CyberSecurity for Networks during the application's life cycle (please refer to the application life cycle page ↗). Before contacting Technical Support, please read the technical support rules ↗.

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

- visit Technical Support website ↗
- Send a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal ↗

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount ↗ is a portal for organizations that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky experts via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky experts and store a history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single user account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

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

- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

Collecting information for Technical Support

Kaspersky Technical Support experts may request your logs from Kaspersky Industrial CyberSecurity for Networks and other system data.

Logs are located on computers that have components of Kaspersky Industrial CyberSecurity for Networks installed. Information about the folders used for storing logs is provided in the Folders for storing application data article.

Root privileges in the operating system are required for providing access to logs.

Kaspersky Technical Support experts may also request additional data on the application components. This data can be obtaining by using the application components centralized installation script named kics4net-deploy-<application version number>.bundle.sh or by locally running the kics4net-gather-artefacts.sh script, which is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

To get information about application components by using the kics4net-deploy-<application version>.bundle.sh script:

1. On the computer from which the centralized installation performed, go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

2. Enter the following command:

   ```
   bash kics4net-deploy-<application version number>.bundle.sh --gather-artefacts -<parameter> <folder name>
   ```

   where:

   - `<parameter>` – determines the data acquisition mode.

     The following parameters are provided:

     - `a` – receive all data.
     - `c` – receive data on certificates.
     - `i` – receive data on the Intrusion Detection configuration.
     - `t` – receive traffic dump files.

   - `<folder name>` – name of the folder used for copying archived data files.

     Example:

     ```
     bash kics4net-deploy-<application version number>.bundle.sh --gather-artefacts -a /tmp/data_for_support
     ```

3. In the `SSH password` and `BECOME password` prompts, enter the password for the user account that was used to run the installation of application components.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh. Upon successful completion, files will be created in the specified folder.

To obtain data on the application component installed on a computer by using the kics4net-gather-artefacts.sh script:

1. Log in to the system using the account credentials of a user account with root privileges.
2. Go to the /opt/kaspersky/kics4net/sbin/ folder and enter the following command for running the script to receive data on an application component:

   ```
   bash kics4net-gather-artefacts.sh -<parameter> <folder name>
   ```

   where:

   - `<parameter>` – determines the data acquisition mode.

     The following parameters are provided:

     - `a` – receive all data.
     - `c` – receive data on certificates.
     - `i` – receive data on the Intrusion Detection configuration.
     - `t` – receive traffic dump files.
   - `<folder name>` – name of the folder used for copying archived data files.

     Example:

     ```
     bash kics4net-gather-artefacts.sh -a /tmp/data_for_support
     ```

   Wait for the kics4net-gather-artefacts.sh script to finish. Upon successful completion, files will be created in the specified folder.

Sources of information about the application

On the Kaspersky Industrial CyberSecurity for Networks page, you can view general information about the application, its functions and features.

The Online Help Guide contains information on administration of Kaspersky Industrial CyberSecurity for Networks. The Online Help Guide also provides information about the application's capabilities that users can utilize to accomplish common tasks.

Online Help includes documentation for the Kaspersky Industrial CyberSecurity for Networks API. This documentation serves as the Developer Guide for the Kaspersky Industrial CyberSecurity for Networks API. In the Kaspersky Industrial CyberSecurity for Networks API Developer Guide, you can find information on performing the following tasks:

- Preparing to use Kaspersky Industrial CyberSecurity for Networks API.
- Handling requests for receiving data from Kaspersky Industrial CyberSecurity for Networks and for sending data to the application.

If you cannot find a solution to an issue on your own, please contact Kaspersky Technical Support.

Appendices

This section provides information that complements the main document text with examples, reference information, and additional data.

Steps to fix the CVE-2024-23836 vulnerability in the Intrusion Detection System

When using the rule-based Intrusion Detection method, the Intrusion Detection System, which is susceptible to the CVE-2024-23836 vulnerability, operates on the nodes with the application components installed. Following the recommendations of the Intrusion Detection System vendor, to quickly fix the specified vulnerability in Kaspersky Industrial CyberSecurity for Networks, disable the SMTP and HTTP protocol processing modules for the intrusion detection rules. The module disabling procedure must be performed on all nodes with the application components installed (Server and sensors).

To disable the SMTP and HTTP protocol processing modules on a node:

1. Open the operating system console.

2. Open the configuration file for the Filter process. To do so, enter the following command:

   ```
   sudo mcedit /var/opt/kaspersky/kics4net/config/Filter.json
   ```

3. Go to the "additionalSuricataArguments" settings section.

4. Add a trailing character `,` (comma) at the end of the line with the last section parameter and below it add the following lines:

   ```
   "--set",
   "app-layer.protocols.smtp.enabled=no",
   "--set",
   "app-layer.protocols.http.enabled=no"
   ```

   Example contents of this section:

   ```
   "additionalSuricataArguments" :
   [
   "--set",
   "runmode=autofp",
   "--set",
   "autofp-scheduler=hash",
   "--set",
   "vars.address-groups.SCAN_HOSTS=0.0.0.0",
   "--set",
   "vars.address-groups.BRUTE_HOSTS=0.0.0.0",
   "--set",
   "app-layer.protocols.smtp.enabled=no",
   "--set",
   "app-layer.protocols.http.enabled=no"
   ]
   ```

5. Save and close the configuration file.

6. Restart the application service. To do so, enter the following command:

   ```
   sudo systemctl restart kics4net.service
   ```

Configuring time synchronization via the NTP and PTP protocols

The time on nodes that have Kaspersky Industrial CyberSecurity for Networks components installed must be synchronized with a common source of time used by industrial network devices. For synchronization purposes, you can use the standard protocols known as Network Time Protocol (NTP) and Precision Time Protocol (PTP).

On the Server node, you must configure time synchronization regardless of how this component was installed (after centralized installation as well as after local installation).

On nodes hosting installed sensors, you must configure time synchronization in the following cases:

- Automatic time synchronization between the Server and sensors was not enabled during centralized installation of Kaspersky Industrial CyberSecurity for Networks.
- The sensor was installed locally using the kics4net-install.sh script.

The steps required for configuring time synchronization may differ depending on the version of the operating system and the specific protocol.

- **Configuring time synchronization via the NTP protocol in CentOS**

  1. Open the operating system console.
  2. Check the status of the standard time synchronization service known as chrony. To do so, enter the following command:
     ```
     systemctl status chronyd
     ```
  3. If the service is not found, enter the following commands to add the package and enable the service:
     ```
     sudo dnf install chrony
     sudo systemctl enable chronyd
     sudo systemctl start chronyd
     ```
  4. Open the service configuration file. To do so, enter the following command:
     ```
     sudo mcedit /etc/chrony.conf
     ```
  5. Specify the NTP servers that will be used for time synchronization. To specify the server, you only need to add the following string:
     ```
     server <server name or IP address> iburst
     ```
  6. Save and close the configuration file.
  7. Restart the service. To do so, enter the following command:
     ```
     sudo systemctl restart chronyd
     ```
  8. Verify that the specified NTP servers are on the list of synchronization sources. To do so, enter the following command:
     ```
     chronyc sources
     ```

- **Configuring time synchronization via the PTP protocol in CentOS**

1. Open the operating system console.

2. Check whether the linuxptp package is installed. To do so, enter the following command:

   ```
   dnf list installed
   ```

3. If the linuxptp package is not installed, enter the following commands to add the package and enable the ptp4l time synchronization service:

   ```
   sudo dnf install linuxptp
   sudo systemctl enable ptp4l
   sudo systemctl start ptp4l
   ```

4. Open the service configuration file. To do so, enter the following command:

   ```
   sudo mcedit /etc/ptp4l.conf
   ```

5. Enter `1` for the `slaveOnly` parameter.

6. Save and close the configuration file.

7. Open the file containing the general settings for the service. To do so, enter the following command:

   ```
   sudo mcedit /etc/sysconfig/ptp4l
   ```

8. In the `OPTIONS` string, specify the parameters as follows:

   ```
   OPTIONS="-f <configuration file> -i <interface name> -S -s"
   ```

   where:

   - `-f <configuration file>` – default name and full path of the configuration file.
   - `-i <interface name>` – name of the network interface that is used for time synchronization.
   - `-S` – enables use of software-based timestamps. You can skip this parameter if you want to use hardware-based timestamps. However, first make sure that the equipment supports this capability.
   - `-s` – enables subordinate time synchronization.

   Example `OPTIONS` string:

   ```
   OPTIONS="-f /etc/ptp4l.conf -i eth0 -S -s"
   ```

9. Save and close the general settings file.

10. Allow use of ports 319 and 320 in the firewall for the UDP protocol. To do so, enter the following commands:

    ```
    sudo firewall-cmd --permanent --add-port=319/udp
    sudo firewall-cmd --permanent --add-port=320/udp
    ```

11. Restart the firewall service. To do so, enter the following command:

    ```
    sudo systemctl restart firewalld
    ```

12. Restart the time synchronization service. To do so, enter the following command:

    ```
    sudo systemctl restart ptp4l
    ```

Supported ASDU types identification in protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards

This article presents the ASDU types identification that are supported in Kaspersky Industrial CyberSecurity for Networks (see the table below). The listed types of frames are processed during Deep Packet Inspection on devices that interact over protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards.

Types of frames in protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards

Frame type ID	Operation	Description	Type of main value / system commands
		1. Process information in the monitoring direction	
<1>	M_SP_NA	Single-point information	bool (0 – OFF, 1 – ON)
<2>	M_SP_TA	Single-point information (with time tag)	bool (0 – OFF, 1 – ON)
<3>	M_DP_NA	Double-point information	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<4>	M_DP_TA	Double-point information (with time tag)	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<5>	M_ST_NA	Step position information	int8 (-64 ... +64)
<6>	M_ST_TA	Step position information (with time tag)	int8 (-64 ... +64)
<7>	M_BO_NA	String of 32 bits	unsigned int32
<8>	M_BO_TA	String of 32 bits (with time tag)	unsigned int32
<9>	M_ME_NA	Measured value, normalized value	float
<10>	M_ME_TA	Measured value, normalized value (with time tag)	float
<11>	M_ME_NB	Measured value, scaled value	float
<12>	M_ME_TB	Measured value, scaled value (with time tag)	float
<13>	M_ME_NC	Measured value, short floating point number	float
<14>	M_ME_TC	Measured value, short floating point number (with time tag)	float
<15>	M_IT_NA	Integrated total	int32
<16>	M_IT_TA	Integrated total (with time tag)	int32
<17>	M_EP_TA	Event of protection equipment (with time tag)	unsigned int8 (0 – Indeterminate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<18>	M_EP_TB	Packed start events of protection equipment (with time tag)	unsigned int8 (Set of bits in accordance with the standard)
<19>	M_EP_TC	Packed output circuit information of protection equipment (with time tag)	unsigned int8 (Set of bits in accordance with the standard)
<20>	M_PS_NA	Packed single-point information with status change detection	unsigned int16
<21>	M_ME_ND	Measured value, normalized value without quality descriptor	float
<30>	M_SP_TB	Single-point information (with time tag CP56Time2a)	bool (0 – OFF, 1 – ON)
<31>	M_DP_TB	Double-point information (with time tag CP56Time2a)	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<32>	M_ST_TB	Step position information (with time tag CP56Time2a)	int8 (-64 ... +64)
<33>	M_BO_TB	String of 32 bits (with time tag CP56Time2a)	unsigned int32
<34>	M_ME_TD	Measured value, normalized value (with time tag CP56Time2a)	float

<35>	M_ME_TE	Measured value, scaled value (with time tag CP56Time2a)	float
<36>	M_ME_TF	Measured value, short floating point number (with time tag CP56Time2a)	float
<37>	M_IT_TB	Integrated totals (with time tag CP56Time2a)	int32
<38>	M_EP_TD	Event of protection equipment (with time tag CP56Time2a)	unsigned int8 (0 – Indeterminate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<39>	M_EP_TE	Packed start events of protection equipment (with time tag CP56Time2a)	unsigned int8 (Set of bits in accordance with the standard)
<40>	M_EP_TF	Packed output circuit information of protection equipment (with time tag CP56Time2a)	unsigned int8 (Set of bits in accordance with the standard)
2. Process information in the control direction			
<45>	C_SC_NA	Single command	bool (0 – OFF, 1 – ON)
<46>	C_DC_NA	Double command	unsigned int8 (0 – Unallowed, 1 – OFF, 2 – ON, 3 – Unallowed)
<47>	C_RC_NA	Regulating step command	unsigned int8 (0 – Unallowed, 1 – Next step UP, 2 – Next step DOWN, 3 – Unallowed)
<48>	C_SE_NA	Setpoint command, normalized value	float
<49>	C_SE_NB	Setpoint command, scaled value	float
<50>	C_SE_NC	Setpoint command, short floating point number	float
<51>	C_BO_NA	String of 32 bits	int32
<58>	C_SC_TA	Single command (with time tag CP56Time2a)	bool (0 – OFF, 1 – ON)
<59>	C_DC_TA	Double command (with time tag CP56Time2a)	unsigned int8 (0 – Unallowed, 1 – OFF, 2 – ON, 3 – Unallowed)
<60>	C_RC_TA	Regulating step command (with time tag CP56Time2a)	unsigned int8 (0 – Unallowed, 1 – Next step UP, 2 – Next step DOWN, 3 – Unallowed)
<61>	C_SE_TA	Setpoint command, normalized value (with time tag CP56Time2a)	float
<62>	C_SE_TB	Setpoint command, scaled value (with time tag CP56Time2a)	float
<63>	C_SE_TC	Setpoint command, short floating point number (with time tag CP56Time2a)	float
<64>	C_BO_TA	String of 32 bits (with time tag CP56Time2a)	int32
3. System information in the monitoring direction			
<70>	M_EI_NA	End of initialization	END OF INITIALIZATION system command
4. System information in the control direction			
<100>	C_IC_NA	Interrogation command	INTERROGATION system command
<101>	C_CI_NA	Counter interrogation command	COUNTER INTERROGATION system command
<102>	C_RD_NA	Read command	READ system command
<103>	C_CS_NA	Clock synchronization command	CLOCK SYNCHRONIZATION system command
<104>	C_TS_NA	Test command	TEST system command
<105>	C_RP_NA	Reset process command	RESET PROCESS ACTIVATION / RESET PROCESS CONFIRMATION system commands
<106>	C_CD_NA	Delay acquisition command	DELAY ACQUISITION system command
<107>	C_TS_TA	Test command (with time tag CP56Time2a)	TEST WITH TIME TAG system command
5. Parameters in the control direction			
<110>	P_ME_NA	Parameter of measured value, normalized value	float
<111>	P_ME_NB	Parameter of measured value, scaled value	float
<112>	P_ME_NC	Parameter of measured value, short floating point number	float

<113>	P_AC_NA	Parameter activation	PARAMETER ACTIVATION system command
6. File transfer			
<120>	F_FR_NA	File ready	Not processed
<121>	F_SR_NA	Section ready	Not processed
<122>	F_SC_NA	Call directory, select file, call file, call section	CALL DIRECTORY, SELECT FILE, CALL FILE, CALL SELECTION system command
<123>	F_LS_NA	Last section, last segment	Not processed
<124>	F_AF_NA	ACK file, ACK section	Not processed
<125>	F_SG_NA	Segment	Not processed
<126>	F_DR_TA	Directory	Not processed

Sending Kaspersky Industrial CyberSecurity for Networks events to SIEM systems

In Kaspersky Industrial CyberSecurity for Networks, you can use a connector to send data to a SIEM system server. After you add a connector, you need to configure forwarding of events through this connector.

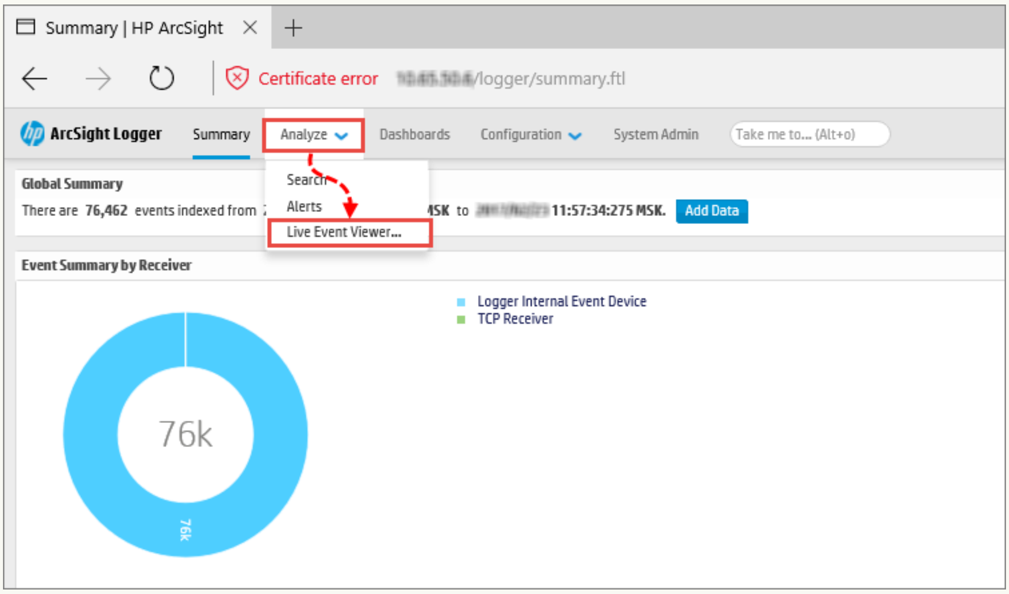
The contents and order in which information is displayed about events forwarded to a SIEM system may differ from the data displayed on the **Events and incidents** tab in the **Events** section of the Kaspersky Industrial CyberSecurity for Networks Server web interface.

- Verifying event forwarding using an HP ArcSight system (as an example)

1. Make sure that a channel is configured for receiving messages from Kaspersky Industrial CyberSecurity for Networks using the standard tools of the HP ArcSight system.

2. Open your browser and enter the address of your HP ArcSight system.

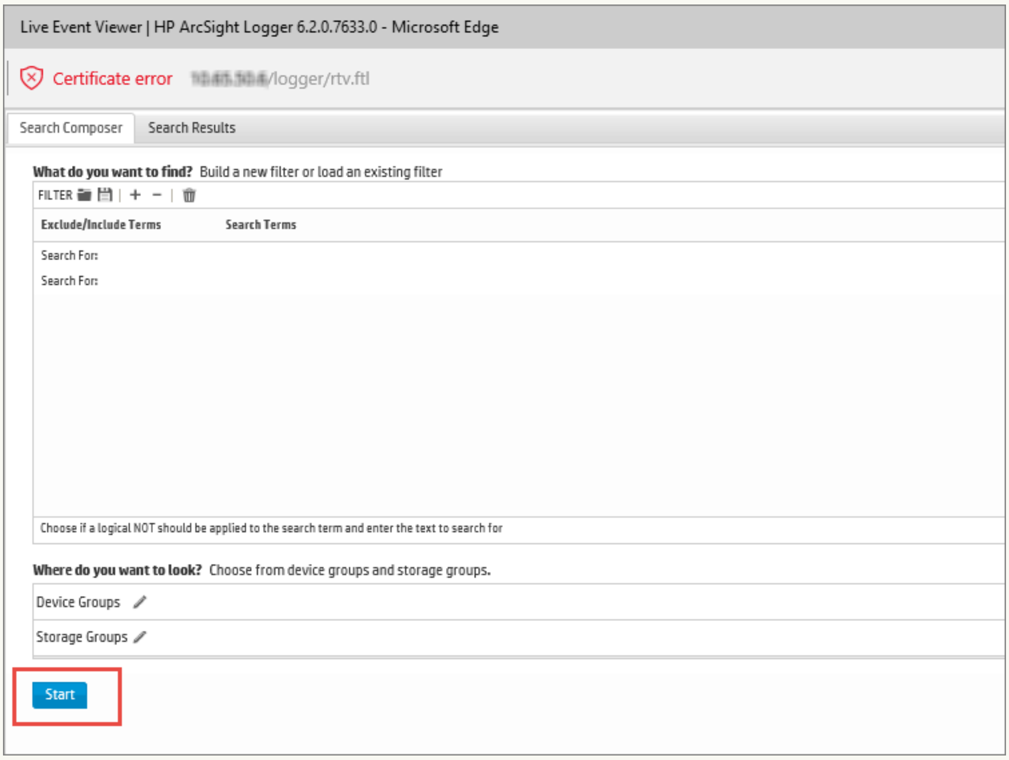
3. Log in to your user account and go to **Analyze** → **Live Event Viewer** (see the figure below).



There are 76,462 events indexed from ... MSK to [redacted] 11:57:34:275 MSK.

Opening the **Live Event Viewer** section in the HP ArcSight system

4. Click the **Start** button (see the figure below).



What do you want to find? Build a new filter or load an existing filter

Choose if a logical NOT should be applied to the search term and enter the text to search for

Where do you want to look? Choose from device groups and storage groups.

Starting **Live Event Viewer** in the HP ArcSight system

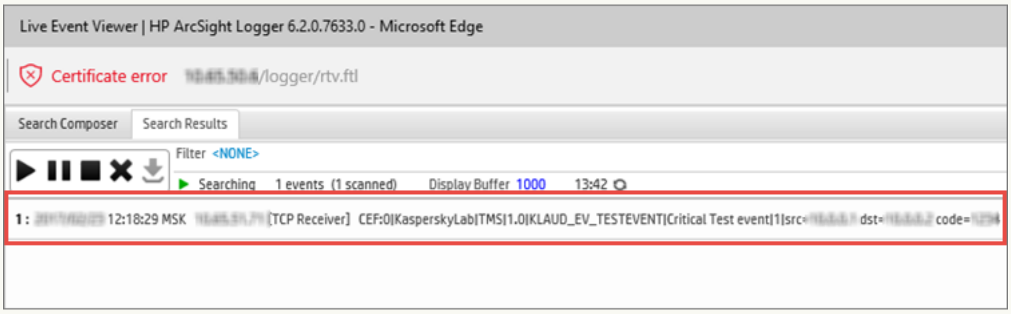
5. Open the command line interface and enter the following command to connect to the server over the Telnet protocol:

```
telnet <ArcSight server address> <port>
```

6. Send a test message in CEF format:

```
CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=10.0.0.1
dst=10.0.0.2 code=1234
```

If there is a connection with the HP ArcSight system, the **Live Event Viewer** section will show an event whose contents match the message that was sent (see the figure below).



```
1 : [redacted] 12:18:29 MSK [redacted] [TCP Receiver] CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=[redacted] dst=[redacted] code=[redacted]
```

Verifying operation results

- [Format of messages forwarded to a SIEM system](#)

The application transmits data to a SIEM system in CEF 20 format. The following internal structures are used for data transmission:

- `EventMessage` – for events.
- `ApplicationMessage` – for application messages.
- `AuditMessage` – for audit entries.

Received messages are not converted to the system log protocol format.

Format of the EventMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Event — corresponding field of the event in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Event	Description
dateTime	Start	Date and time (with precision down to the millisecond) when the event-triggering network packet was captured.
hostname	Kaspersky Industrial CyberSecurity for Networks Server address	Address of the Kaspersky Industrial CyberSecurity for Networks Server.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.1.0.463	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Event	Sent message type.
signatureId	Event type	Event type ID.
name	Title	Event description.
severity	Event severity level: • 9 – scores 8.0–10.0 • 6 – scores 4.0–7.9 • 3 – scores 0.0–3.9	Event severity level. Values from 3 to 9, where 9 is the most severe event.
score	Event score	Event score value.
extension	Indicated in the Extension Fields table	Determined individually for each type of message.

Date and time is sent in the following format: `YYYY-MM-DD`T`hh:mm:ss.ms`Z. Example: 2023-09-30T22:14:15.030Z – time of the event, which occurred on September 30, 2023 at 22 hours, 14 minutes, 15 seconds, and 030 milliseconds.

Contents of Extension Fields

The table below provides data in the following columns:

- Extension — field name in a message.
- Related events — events in which the specific field is sent.
- Description — field description.

Extension	Related events	Description
cnt	Common fields of events	Counter of the number of times an event is repeated after the event is registered.
dmac	Common fields of events	Destination MAC address.
dmacas	Common fields of events	Address space for the destination MAC address.
dpt	Common fields of events	Destination port.
dst	Common fields of events	Destination IP address.
das	Common fields of events	Address space for the destination MAC address (if additional address spaces are added to the application).
end	Common fields of events	Event end time.
smac	Common fields of events	Source MAC address.
smacas	Common fields of events	Address space for the source MAC address.
spt	Common fields of events	Source port.
src	Common fields of events	Source IP address.
srcas	Common fields of events	Address space for the source MAC address (if additional address spaces are added to the application).
start	Common fields of events	Event registration time.
technology	Common fields of events	Technology that was used to register the event.
triggeredRule	Common fields of events	Triggered rule.
protocol	Common fields of events	Protocol.
vlanId	Common fields of events	VLAN ID.
monitoringPoint	Common fields of events	Monitoring point whose traffic invoked registration of the event.
sourceIndustrialAddress	Common fields of events	Application-level address for the source.
destinationIndustrialAddress	Common fields of events	Application-level address for the destination.
eventIdentifier	Common fields of events	Event ID.
noTrafficDuration	No traffic at monitoring point	Period of no traffic.
tagId	Invalid tag type	Tag ID.
expectedTagType	Invalid tag type	Expected data type of tag.
actualTagType	Invalid tag type	Actual data type of tag.
ruleName	• Process Control rule violation • Intrusion Detection rule from the system set of rules was triggered	Rule name.
tags	Process Control rule violation	Tags.
msg	Intrusion Detection rule from the system set of rules was triggered	Message.
substitutedIpAddress	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	IP address of the source of network packets.

targetIpAddress	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	IP address of the destination of network packets.
attackStartTimestamp	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	Start time of the activity showing signs of an attack.
ownerMac	• IP address conflict detected • New IP address detected • New device detected • New information received • Traffic detected from MAC address • MAC address added to device • IP address added to device	MAC address of owner.
ownerIp	• New device detected • MAC address added to device • IP address added to device • IP address conflict detected • New MAC address detected	IP address of owner.
challengerMac	IP address conflict detected	MAC address of challenger.
newIpAddress	New IP address detected	New IP address.
newMacAddress	New MAC address detected	New MAC address.
oldIpAddress	New IP address detected	Old IP address.
assetName	New device detected	Device name.

Device settings

The table below provides data on the settings of devices.

If one or two devices were identified for a detected interaction, Kaspersky Industrial CyberSecurity for Networks also sends known information about one or two devices to the SIEM system.

If multiple devices were identified for a detected interaction, the message is duplicated with different address information and different device settings (if the devices are different).

Extension	Device setting
srcAssetName	Name of the source device.
srcVendor	Vendor of the source device.
srcOS	Operating system of the source device.
srcNetworkName	Network name of the source device.
srcModel	Model of the source device.
dstAssetName	Name of the destination device.

dstVendor	Vendor of the destination device.
dstOS	Operating system of the destination device.
dstNetworkName	Network name of the destination device.
dstModel	Model of the destination device.

Format of the ApplicationMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Application message – corresponding field of the application messages in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Application message	Description
dateTime	Occurrence date and time	Date and time (to the millisecond) when the situation that caused the message logging was detected.
hostname	Address of Kaspersky Industrial CyberSecurity for Networks Server or sensor	Node address of Kaspersky Industrial CyberSecurity for Networks Nodes Server or sensor.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.1.0.463	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Application message	Sent message type.
severity	Application messages severity level: • 10 for the following statuses: *Moderate malfunction*, *Critical malfunction* or *Fatal malfunction*. • 5 for the following statuses: *Unknown*, *Malfunction*. • 0 for the *Normal operation* status.	Application messages severity level. Values from 0 to 10, where 10 is the most severe message.
address	Node address	Address of the node from which the message originated.
systemProcess	Process name	Application process that invoked message registration.
msg	Message	Numerical identifier and text of the message.

Format of the AuditMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Audit message – corresponding field of the audit entry in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Audit message	Description

dateTime	Occurrence date and time	Date and time (to the millisecond) when the situation that caused the audit entry logging was detected.
hostname	Kaspersky Industrial CyberSecurity for Networks Server address	Node address of Kaspersky Industrial CyberSecurity for Networks Server.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.1.0.463	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Audit message	Sent message type.
address	User node	Address of the node where the registered action was performed.
user	User	Name of the user that performed the registered action.
action	Action	Registered action performed by the user.
result	Result	Result of the registered action (successful or unsuccessful).
msg	Description	Additional information about the registered action.

Specifics of connecting Kaspersky Industrial CyberSecurity for Networks nodes as connection gateways in Kaspersky Security Center

You can use nodes with installed application components (Server and sensors) as connection gateways in Kaspersky Security Center. Distribution points act as gateways for connections to the Kaspersky Security Center Administration Server. The diagram of communication with managed devices using distribution points allows you to optimize database, application module, and Kaspersky Lab application update traffic on the network and configure traffic restrictions for IP ranges in Kaspersky Security Center. If a Kaspersky Industrial CyberSecurity for Networks Server or sensor node provides the only available connection between the Administration Server and managed devices located on an isolated network, the connection gateway role on this node allows you to provide Administration Server network connectivity with these devices.

This article describes a scenario for configuring and scanning a Kaspersky Industrial CyberSecurity for Networks node to act as a connection gateway in Kaspersky Security Center. The scenario consists of the following steps:

1. **Installing Network Agent on the node**

   Network Agent is installed automatically on the Kaspersky Industrial CyberSecurity for Networks Server node if the functionality for communication between the application and Kaspersky Security Center was added during Server installation. After adding the communication functionality, enable and configure the functionality in Kaspersky Industrial CyberSecurity for Networks.

   You must enable and configure the communication functionality in Kaspersky Industrial CyberSecurity for Networks before configuring Network Agent on the Server to act as a connection gateway. Enabling the communication functionality after configuring Network Agent on the Server resets the specified configuration settings and disables the connection gateway role on the node. In that case, to resume node operation as a connection gateway, repeat the steps in the scenario, starting with Network Agent configuration.

   Network Agent is not installed by default on the sensor node. To install Network Agent from the current application version distribution kit, do the following on the computer with the sensor installed:

1. Copy the package file for installing Network Agent from the directory with the unpacked script and installation package files included in the distribution kit to an arbitrary directory. The file is located in the kics4net-release_<application version>/linux-centos subfolder. File name: klnagent64-<Network Agent version number>.x86_64.rpm.

2. In the operating system console, go to the folder containing package file, and enter the following command:

   ```
   sudo rpm -i klnagent64-< Network Agent version number >.x86_64.rpm
   ```

Wait for the Network Agent installation process to finish.

2 Allowing the use of ports

At this step, you must allow the use of firewall ports on the Network Agent node computer. You can use the following commands to enable port use:

```
sudo firewall-cmd --permanent --add-port=13000/tcp
```

```
sudo firewall-cmd --permanent --add-port=13295/tcp
```

```
sudo systemctl restart firewalld
```

3 Configuring Network Agent

This step activates connection gateway mode on Administration Agent. When this mode is activated with subsequent addition of a node as a distribution point, Kaspersky Security Center changes the identification and authentication details for using this device as a connection gateway.

Changes to credentials and authentication information require that for the new distribution point to be used as the connection gateway ↗ on a previously configured network, you reinstall Network Agent on all devices that you want to connect to the newly added connection gateway. This includes those devices that previously used the node as a connection gateway. Until Network Agent is reinstalled on these devices, they will not be able to connect to the newly added connection gateway.

To activate connection gateway mode on Network Agent, you need to perform the following actions on the node computer:

1. Run the post-installation script to configure the Network Agent local environment. To do so, enter the following command:

   ```
   sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

2. Please carefully read the End User License Agreement. To go to the next screens containing the text of the End User License Agreement, press **SPACE**.

3. When done viewing and if you fully agree with the terms of the End User License Agreement, accept the terms. To do so, enter `y`.

4. Enter the Administration Server name or IP address.

5. If needed, change the default ports for unencrypted and encrypted connections to the Administration Server.

6. Select a mode for connecting to the Administration Server. To do so, enter the appropriate character:

   `y`: secure connections via SSL

   `n`: unencrypted connections.

7. At the step where the Network Agent operation mode is requested, select **Use as connection gateway**.

8. Wait for the script to finish. Two to three minutes after the script finishes running, check the connection between Network Agent and the Administration Server. To do so, enter the following command:

   ```
   sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

The screen will display information about the connection to the Administration Server. If the configuration was applied successfully, the following messages will be displayed on the screen:

```
HostId: < ID as an alphanumeric sequence >

This host was installed as a connection gateway, but not yet registered on server

Connecting to server...OK

Connecting to the Administration Agent...OK
```

4 Adding a node as a distribution point in Kaspersky Security Center

The Kaspersky Industrial CyberSecurity for Networks node will begin acting as a connection gateway after it is added as a distribution point in Kaspersky Security Center. To do this, do the following:

1. Kaspersky Security Center Administration Server.

2. In the console tree, open the context menu of the **Administration Server** node and select **Properties**.

3. In the Administration Server properties window, select the **Distribution points** section.

4. In the right part of the window, select **Manually assign distribution points** and click **Add**.

   The **Add distribution point** window opens.

5. To specify a device that will act as a distribution point, select the option to add a connection gateway and enter the IP address or computer name of the Kaspersky Industrial CyberSecurity for Networks node.

6. To specify the scope of the distribution point, select the **Administration group** option and specify the administration group whose devices will use the connection gateway.

7. After adding the node to the list of distribution points, make sure that a persistent connection with the Administration Server is enabled for the node. To do so, open the node properties window and check that the **Do not disconnect from the Administration Server** check box in the **General** section is selected. This check box must be selected automatically and must not be cleared or selected manually.

5 Verifying a successful connection between Network Agent and Kaspersky Security Center

You can verify that the steps involved in adding the connection gateway and distribution point were successful on the node computer. To do so, enter the following command:

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

The screen will display information about the connection to the Administration Server. If the steps are completed successfully, the following messages are displayed on the screen:

```
Host is a connection gateway

Host is a distribution point

Connection with server: active

CG connection with server: active
```

Files for importing a universal project

You can use a universal-format project to import Process Control configurations for devices and tags into Kaspersky Industrial CyberSecurity for Networks. A universal project can be imported by using text files with delimiters (CSV files). CSV format is a text format for presentation of table data.

You can create data files using any method of your choice (for example, from SCADA systems). To import your created files into the application, you need to pack the files into a ZIP archive.

The set of files used for importing a universal project may consist of the following CSV files:

- devices.csv. Contains descriptions of devices.
- connections.csv. Contains descriptions of connections.

  A *connection* is a named link between a device, a set of device protocols, and a set of device tags relayed through such protocols.
- variables.csv. Contains descriptions of variables and tags for connections.
- enums.csv. Contains descriptions of enumerations for the IEC 61850 standard.
- datasets.csv. Contains descriptions of data sets for the IEC 61850 standard.
- iec61850_mms_reports.csv. Contains descriptions of reports for the IEC 61850: MMS protocol.

When using data files, consider the following specifics:

- Data files must have UTF-8 encoding.
- The list of tags in the variables.csv file has the "connection" grouping attribute.
- You can specify several different protocols and addresses for one connection in the connections.csv file.
- A protocol can have one or several addresses.
- One device can have several connections with different sets of tags.

Rows containing the parameter values in the enums.csv and datasets.csv files are filled out only when describing enumerations and data sets for MMS and GOOSE protocols of the IEC 61850 standard. For other protocols, the enums.csv and datasets.csv files can contain only header rows. Please note that the enums.csv and datasets.csv files must be included in the set of files used for the import.

When data files are imported, only the values of the specified parameters are considered. Parameters whose values are not specified are omitted. If the data file is missing strings to which a different file from the set of data files contains references, the relevant strings are omitted during import.

File with descriptions of devices: devices.csv

The file with descriptions of devices contains an enumeration of devices, their types, and connection IDs. Connection ID in the device description file is specified in the connections description file and is used for linking protocols to the devices.

If you use different protocols with different sets of tags, you have to use several connections for one device. Connection IDs in each row of the devices.csv file have to be unique.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the devices.csv file is provided below.

Example:

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Device;Type;Connection
```

Header strings of the devices.csv file contain the following values:

- `Devices`

  The name of the CSV file is specified in this string. `Devices` – the name of the device description file. The data file name corresponds to the file purpose and is defined for each file in the set.

- `Format Version;KICS Importer Version`

  This string specifies the version of the file format and the version of the tool using which the file was created. Specify the value V1.0.0.0 for the parameter `Format version`. It is then recommended to specify the name and version of the tool that was used to create the CSV file.

- `Field separator: ; Decimal separator: . Text quotes: " Var name separator: .`

  Use this string to specify the separators used in the data file:

  - `Field separator: ;`
  - `Decimal separator: .`
  - line terminator: `Text quotes: "`
  - field separator in tag name: `Var name separator: .`

- `Device;Type;Connection`

  This string contains the names of columns with data. Data in the file should be arranged according to the following order of columns:

  - `Device` – device name.
  - `Type` – device type code. The following codes are used:
    - 0 – SIEMENS SIMATIC S7-300
    - 1 – SIEMENS SIMATIC S7-400
    - 2 – SCHNEIDER ELECTRIC MOMENTUM
    - 3 – SCHNEIDER ELECTRIC M340
    - 4 – MITSUBISHI SYSTEM Q
    - 5 – ALLEN-BRADLEY CONTROL LOGIX 5000
    - 6 – SIEMENS SIPROTEC
    - 7 – IEC 61850 GOOSE, MMS device
    - 8 – IEC 60870-5-104 device

- 9 – ABB RELION 670
- 10 – GENERAL ELECTRIC RX3I
- 11 – SIEMENS SIMATIC S7-1500
- 12 – IEC 61850 SAMPLED VALUES device
- 13 – SIEMENS SIPROTEC 6MD66
- 14 – SIEMENS SIPROTEC 7SS52
- 15 – SIEMENS SIPROTEC 7UM62
- 16 – SIEMENS SIPROTEC 7SA52
- 17 – SIEMENS SIPROTEC 7SJ64
- 18 – SIEMENS SIPROTEC 7UT63
- 19 – GENERAL ELECTRIC MULTILIN B30
- 20 – GENERAL ELECTRIC MULTILIN C60
- 21 – EMERSON DELTAV
- 22 – SCHNEIDER ELECTRIC M580
- 23 – RELEMATIKA TOR 300
- 24 – EKRA 200 series
- 25 – EKRA BE2704 / BE2502
- 26 – OMRON CJ2M
- 27 – ABB AC 800M
- 28 – YOKOGAWA CENTUM
- 29 – CODESYS V3 based device
- 30 – DNP3 device
- 31 – OPC UA server
- 32 – ABB AC 700F
- 33 – SIEMENS SIMATIC S7-1200
- 34 – OPC DA server
- 35 – BECKHOFF CX series
- 36 – PROSOFT-SYSTEMS REGUL R500

- 37 – EMERSON CONTROLWAVE
- 38 – IEC 60870-5-101 device
- 39 – MOXA NPORT IA 5000 series
- 40 – I/O device
- 41 – ABB RELION REF615
- 42 – SIEMENS SIMATIC S7-200
- 43 – MODBUS TCP device
- 44 – SCHNEIDER ELECTRIC SEPAM 80 NPP
- 45 – YOKOGAWA PROSAFE-RS
- 46 – SCHNEIDER ELECTRIC FOXBORO FCP280 / FCP270
- 47 – HONEYWELL CONTROLEDGE 900 series
- 48 – HONEYWELL EXPERION C300
- 49 – SCHNEIDER ELECTRIC MICOM C264
- 50 – UMAS device
- 51 – TASE.2 server
- 52 – PROFINET device
- 53 – DIRECTLOGIC
- 54 – Server with encryption support
- 55 – BACNET device
- 56 – SCHNEIDER ELECTRIC P545
- 57 – YCU/ELC
- 58 – FEU device
- 59 – Generic IED
- 60 – Generic Gateway
- 61 – Generic PLC
- 62 – VALMET DNA device
- 63 – IPU device
- 64 – OWEN PLC100 series

  - 65 – CODESYS V2 based device
  - 66 – PNU20 device
  - 67 – KNX device
  - 68 – DTS device
  - 69 – B&R
  - 70 – SIEMENS SICAM PAS server
- `Connection` – connection ID from the connections.csv file containing a description of connections.

The header strings are followed by the file body containing the values of parameters (device name, device type code, connection ID). An example of the devices.csv file is provided below.

Example:
```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Device;Type;Connection
"ms_plc";4;"ms_plc"
"mc_SysQ";8;"mc_SysQ"
```

Connections description file: connections.csv

A connections description file contains the IDs of connections, codes of application-layer protocols, and full network addresses of devices.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the connections.csv file is provided below.

Example:
```
'Connections

'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0

'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .

'Connection;Protocol;Address
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;Protocol;Address` contains the names of columns with data:

- `Connection` – connection ID for description files.

  Connection ID is used to link protocols to devices and tags.
- `Protocol` – code of the application-level protocol. The following protocol codes are used:
  - 0 – MODBUS TCP
  - 1 – SIEMENS S7COMM over TCP
  - 2 – SIEMENS S7COMM over INDUSTRIAL ETHERNET

- 3 – MITSUBISHI MELSEC SYSTEM Q
- 4 – ALLEN-BRADLEY ETHERNET/IP
- 5 – IEC 61850 MMS
- 6 – IEC 61850 GOOSE
- 7 – IEC 60870-5-104
- 8 – GENERAL ELECTRIC SRTP
- 9 – IEC 61850 SAMPLED VALUES
- 10 – SIEMENS S7COMMPLUS over TCP
- 11 – EMERSON DELTAV
- 12 – OMRON FINS over UDP
- 13 – MMS for ABB AC 800M
- 14 – YOKOGAWA VNET/IP
- 15 – CODESYS V3 GATEWAY over TCP
- 16 – DNP3
- 17 – OMRON FINS over TCP
- 18 – OPC UA BINARY
- 19 – DMS for ABB AC 700F
- 20 – OPC DA
- 21 – OMRON FINS over ETHERNET/IP
- 22 – CODESYS V3 GATEWAY over UDP
- 23 – BECKHOFF ADS/AMS
- 24 – IEC 60870-5-101
- 25 – FOXBORO FCP280 / FCP270 INTERACTION
- 26 – BSAP
- 27 – HONEYWELL CONTROLEDGE 900 INTERACTION
- 28 – WMI INTERACTION
- 29 – HONEYWELL EXPERION INTERACTION
- 30 – MiCOM C264 INTERACTION

  - 31 – SCHNEIDER ELECTRIC UMAS
  - 32 – TASE.2
  - 33 – PROFINET IO
  - 34 – DIRECTLOGIC INTERACTION
  - 35 – BACNET
  - 36 – YARD
  - 37 – COS
  - 38 – IPU-FEU INTERACTION
  - 39 – VALMET DNA INTERACTION
  - 40 – CODESYS V2
  - 41 – PNU20
  - 42 – GENERAL ELECTRIC EGD
  - 43 – KNXnet/IP
  - 44 – DTS
  - 45 – INA2000
  - 46 – SIEMENS SICAM SCC - INTERACTION with SICAM PAS
- `Address` – a string containing the full network address of the device, which is specific to the given protocol.

Example:

Connection with the Schneider Momentum controller (one IP address):

```
"Barline1";0;"IP-Address=192.168.0.7;Port=502"
```

Connection with the Mitsubishi System Q controller (one IP address, two ports):

```
"Station1";3;"IP-Address=192.168.0.8;Port=5001 Network=0;Station=0;PC=255"
"Station1";3;"IP-Address=192.168.0.8;Port=5002 Network=0;Station=0;PC=255"
```

Connection with the redundant Siemens S7-400 controller, two controllers (two IP addresses, one set of tags):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
"S7$Program";1;"IP-Address=192.168.0.22;Port=102;Rack=0;Slot=2"
```

The connection with the Siemens S7-400 controller uses two protocols: S7Comm over the TCP/IP stack, and S7Comm over the Industrial Ethernet network (one set of tags):

```
"S7$Program";1;"IP-Address=192.168.0.21;Port=102;Rack=0;Slot=2"
"S7$Program";2;"MAC=00:01:02:03:04:05;Rack=0;Slot=2"
```

The header strings are followed by the file body containing the values of parameters (connection ID, application-level protocol code, full network address of the device). An example of the connections.csv file is provided below.

Example:

```
'Connections
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;Protocol;Address
"ms_plc";3;"IP-Address=192.168.0.77;Port=1025"
"mc_SysQ";7;"IP-Address=192.168.0.77;Port=2404;Asdu=555"
```

The format of the device network address in the file connections.csv depends on the type of protocol used.

Example:
The following address formats can be used for protocols supported by Kaspersky Industrial CyberSecurity for Networks:

- MODBUS TCP:
  `"IP-Address=192.168.0.7;Port=502"`
- SIEMENS S7COMM over TCP:
  `"IP-Address=192.168.0.7;Port=502;Rack=0;Slot=2"`
- SIEMENS S7COMM over INDUSTRIAL ETHERNET:
  `"MAC=00:01:02:03:04:05;Rack=0;Slot=2"`
- MITSUBISHI MELSEC SYSTEM Q:
  `"IP-Address=192.168.0.7;Port=502;Network=0;Station=0;PC=255"`
- ALLEN-BRADLEY ETHERNET/IP:
  `"IP-Address=192.168.0.7;Port=44818"`
- IEC 61850 MMS:
  `"IP-Address=192.168.0.7;Port=502;Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 61850 GOOSE:
  `"Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 60870-5-104:
  `"IP-Address=192.168.0.7;Port=104;Asdu=2"`
- GENERAL ELECTRIC SRTP:
  `"IP-Address=192.168.0.50;Port=18245"`
- IEC 61850 SAMPLED VALUES:
  `"MAC=00:01:02:03:04:05;Domains=IED_TRANSFORMER1;Vendor=TMW;Model=IED"`
- SIEMENS S7COMMPLUS over TCP:
  `"IP-Address=192.168.0.22;Port=102"`
- EMERSON DELTAV:
  `"IP-Address=192.168.0.38;Port=18507"`
- OMRON FINS over UDP:
  `"IP-Address=192.168.0.1;Port=9600"`
- MMS for ABB AC 800M:
  `"IP-Address=192.168.0.60;Port=102"`
- YOKOGAWA VNET/IP:
  `"IP-Address=192.168.0.4;Port=5313"`

- CODESYS V3 GATEWAY over TCP:
  `"IP-Address=192.168.0.4;Port=11740"`

- DNP3:
  `"IP-Address=192.168.1.10;Port=20000"`

- OMRON FINS over TCP:
  `"IP-Address=192.168.0.1;Port=9600"`

- OPC UA BINARY:
  `"IP-Address=192.168.0.213;Port=49320"`

- DMS for ABB AC 700F:
  `"IP-Address=192.168.0.7;Port=9991"`

- OMRON FINS over ETHERNET/IP:
  `"IP-Address=192.168.0.1;Port=44818"`

- OPC DA:
  `"IP-Address=192.168.0.7;Port=135"`

- CODESYS V3 GATEWAY over UDP:
  `"IP-Address=192.168.0.7;Port=1740"`

- BECKHOFF ADS/AMS:
  `"IP-Address=192.168.0.7;Port=48898"`

- IEC 60870-5-101:
  `"IP-Address=192.168.0.7;Port=950"`

- FOXBORO FCP270, FCP280 INTERACTION:
  `"MAC=00:00:6C:C0:00:0A"`

- BSAP:
  `"IP-Address=192.168.0.7;Port=1234"`

- HONEYWELL CONTROLEDGE 900 INTERACTION:
  `"IP-Address=192.168.1.99;Port=41103"`

- HONEYWELL EXPERION INTERACTION:
  `"IP-Address=192.168.1.10;Port=55553"`

- SCHNEIDER ELECTRIC UMAS:
  `"IP-Address=192.168.0.7;Port=502"`

- TASE.2:
  `"IP-Address=192.168.0.20;Port=102"`

- PROFINET IO:

`"MAC=00:01:02:03:04:05;\IP-Address=192.168.0.20;\Frame=IDS_TEL352"`

- DIRECTLOGIC INTERACTION:
  `"IP-Address=192.168.0.70;Port=28784"`
- BACNET:
  `"IP-Address=192.168.5.200;Port=47808"`
- YARD:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.12.1\;Port=2002"`
- COS:
  `"IP-Address=192.168.1.131;Port=3077"`
- IPU-FEU INTERACTION:
  `"IP-Address=192.168.5.200;Port=57005"`
- VALMET DNA INTERACTION:
  `"IP-Address=192.168.10.11;Port=2519"`
- CODESYS V2:
  `"IP-Address=192.168.7.200;Port=1210"`
- PNU20:
  `"IP-Address=192.168.7.200;Port=43962"`
- GENERAL ELECTRIC EGD:
  `"IP-Address=192.168.0.51\;Port=18246"`
- KNXnet/IP:
  `"IP-Address=192.168.10.76;Port=3671"`
- DTS:
  `"IP-Address=192.168.50.11;Port=30000"`
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS:
  `"IP-Address=192.168.50.01;Port=10501"`

File with descriptions of tags and variables: variables.csv

The variables and tags description file contains enumerations of tags, their parameters, and connections with which the tags are linked.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the variables.csv file is provided below.

Example

```
'Variables
```

```
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;E` contains the names of columns with data:

- `Id` – unique numerical ID of the tag.

  The tag ID is needed to create links to the tag in the datasets.csv file.

- `Varname` – full name of the tag (for example, `Drain.8450PT00058.value20`).

- `Connection` – ID of the connection with which the tag is linked.

  Connection ID is specified in the connections description file and is used for linking protocols to tags.

- `Address` – address of the tag in string form.

  The address depends on the type of the protocol with which the tag is linked (for example, for the S7comm protocol the address value is `M2.7`, `DB575:82.0`, and for the Modbus TCP protocol the address value is `400537`, `123`, `300001`).

- `Datatype` – numerical code of the tag data type. The following codes are used:

  - 0 – BOOL
  - 1 – INT8
  - 2 – UINT8
  - 3 – INT16
  - 4 – UINT16
  - 5 – INT32
  - 6 – UINT32
  - 7 – INT64
  - 8 – UINT64
  - 9 – FLOAT
  - 10 – DOUBLE
  - 11 – STRING
  - 12 – ENUM
  - 13 – BOOL ARRAY
  - 14 – UNSPECIFIED

- `Length` – string length in bytes for a tag of the string type.

- `InLo;InHi;OutLo;OutHi` – parameters for scaling the tag value.

  If the values of all parameters for scaling the tag value are equal to zero, scaling of the tag value is not used. If numerical values of parameters are specified, the following formula is used to calculate the tag value: TagValue = OutLo + (TagValue – InLo) * (OutHi – OutLo) / (InHi – InLo), where TagValue is the tag value.

- `Description` – tag description (for example, "Steam pressure at the output of Boiler No. 1").

- `EngUnits` – units of measurement of the physical quantity corresponding to the tag (for example, m/s, J).

- `EnumName` – name of the enumeration from the enums.csv file, which defines the value of the tag.

  The `EnumName` field can be filled for tags with data types ENUM, INT*, or UINT*. The `EnumName` field contains a link to the enumeration from the enums.csv file.

  Example:
  The `EnumName` field in the variables.csv file:
  ```
  EnumName = "OnOffSwitch"
  ```
  Description of the enumeration in the enums.csv file:
  ```
  "OnOffSwitch"; 0; " On "
  "OnOffSwitch"; 1; " Off "
  ```

The header strings are followed by the file body containing the values of parameters (for example, tag ID, tag name, or connection ID). An example of the variables.csv file is provided below.

Example:
```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
5;"System.mitsub_n.ms_plc.Bit01";"ms_plc";"W0";4;0;0;0;0;0;"System.mitsub_n.ms_plc.Bit01";"";""
6;"System.mitsub_n.ms_plc.Register01";"ms_plc";"W20";9;0;0;0;0;0;"System.mitsub_n.ms_plc.Register01";"";""
1;"systemQ.Bit01";"mc_SysQ";"10";0;0;0;0;0;0;"systemQ.Bit01";"";""
```

The structure of the tag address in the `Address` field depends on the protocol used.

The following structure addresses are used for the supported protocols:

- MODBUS TCP: integer (for example, addresses of discrete inputs: from 100001).

- SIEMENS S7COMM over TCP and S7COMM over INDUSTRIAL ETHERNET: string in the format `[Area][ByteAddress].[BitAddress]`.

  If the condition `MemArea=DataBlocks` is satisfied, the address is supplemented with the number of the data block. The string changes to `[DB17]:[ByteAddress].[BitAddress]`, where:

  - `Area` – the enumeration of codes of memory areas according to the protocol standard: M, I, O, DB, C, T.

  - `ByteAddress` – the byte address represented by an integer.

  - `BitAddress` – the bit address inside the byte, which is represented by an integer.

- MITSUBISHI MELSEC SYSTEM Q: a string in the format `[Area][Address]`, where:

  - `Area` – the enumeration of codes of memory areas according to the protocol specification: SM, SD, M, L, F, V, D, TS, TC, TN, SS, SC, SN, CS, CC, CN, S, Z, R, X, Y, B, W, SB, SW, DX, DY, ZR.

  - `Address` – the address value. The address is an integer in the range that depends on the data area.

- ALLEN-BRADLEY ETHERNET/IP: a string with the tag name.

- IEC 61850 MMS and GOOSE: per the IEC 61850 standard – a string of the format `DOMAIN=Domain;LN=LnName;CO=CoName;DA=FullTagName;CDC=CdcName;LNCDC=LNClassName`, where:
  - `DOMAIN` – a parameter that includes the device name and the logical device name.
  - `LN` – logical node name.
  - `CO` – functional constraint name.
  - `DA` – tag name.
  - `CDC` – attribute common data class name.
  - `LNCDC` – logical node common data class name.
- IEC 60870-5-104 and IEC 60870-5-101: a string in the format `[ASDU]:[Address]`, where:
  - `ASDU` – ASDU number represented by an integer.
  - `Address` – InformationObject number represented by an integer.
- GENERAL ELECTRIC SRTP: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` – the enumeration of codes of memory areas according to the protocol standard: I, Q, T, M, G, AI, AQ, R, P, L, W.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- SIEMENS S7COMMPLUS over TCP: string in the format `LID=LidValue;RID=RidValue`, where `LidValue` and `RidValue` are internal identifiers of a tag in the TiaPortal project.
- EMERSON DELTAV: a string with the tag name.
- OMRON FINS over UDP, OMRON FINS over TCP and OMRON FINS over ETHERNET/IP: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` – enumeration of codes of memory areas according to the protocol standard: A, CIO, C, CS, D, DR, E, H, IR, TK, T, TS, W.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- YOKOGAWA VNET/IP: a string with the tag name.
- DNP3: string in the format `[GROUP]:[INDEX]`, where:
  - `GROUP` is the specific group.
  - `INDEX` is the specific index.
- DMS for ABB AC 700F: integer.

- MMS for ABB AC 800M: string in the format `[Application]:[POUInstance].[VarOffset]`, where:
  - `Application` is the name of the application.
  - `POUInstance` is the POU instance.
  - `VarOffset` is the variable offset.
- CODESYS V3 GATEWAY over TCP and CODESYS V3 GATEWAY over UDP: string with the tag name.
- OPC UA BINARY: a string with the tag name.
- OPC DA: a string with the tag name.
- BSAP: string in the format `[MSD_VERSION]:[MSD]`, where:
  - `MSD_VERSION` is an integer in the range of 0–65535 that is used for comparing versions of projects/tags in the PLC and SCADA system.
  - `MSD` is the tag ID represented by an integer in the range of 0–65535.
- FOXBORO FCP280 / FCP270 INTERACTION: string containing the tag name.
- HONEYWELL EXPERION INTERACTION: string in the format `[BLOCK_ID]:[SUBBLOCK_ID]:[PROPERTY_ID]`, where:
  - `BLOCK_ID` is the sequence number of the PLC program block represented by an integer in the range of 0–65,535.
  - `SUBBLOCK_ID` is the sequence number of the PLC program subblock represented by an integer in the range of 0–65,535.
  - `PROPERTY_ID` is the sequence number of the PLC program block parameter represented by an integer in the range of 0–65,535.
- DIRECTLOGIC INTERACTION: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` is the enumeration of memory area codes according to the protocol specification: X, Y, C, S, T, CT, GX, GY, V, P, SP, B, PB.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- BACNET: string in the format `[OBJECT_TYPE]:[OBJECT_ID]`, where:
  - `OBJECT_TYPE` is the type of object according to the protocol specification.
  - `OBJECT_ID` is the sequence number of the object represented by an integer in the range of 0–4,194,303.
- PROFINET IO: string in the format `[IO]:[SubSlot]:[Index]:[Offset].[BitAddress]`, where:
  - `IO` is the variable direction (input, output).
  - `SubSlot` is the number of the subslot represented by an integer.

  - `Index` is the tag index represented by an integer.
  - `Offset` is the tag byte address represented by an integer.
  - `BitAddress` is the bit address inside the byte, which is represented by an integer (used only for tags that have the bool data type).

  In addition, to correctly load the protocol parameters, you must specify the GSDML file for the specific device.

- YARD: string in the format `[Controller Address]:[Index]:[Size]:[Config]:[MessageType]`, where:
  - `Controller Address` – address of the object controller represented by a hexadecimal integer.
  - `Index` – bit tag index represented by an integer.
  - `Size` – bit size represented by an integer.
  - `Config` – position of the jumpers on the object controller represented by a hexadecimal integer.
  - `MessageType` – type of message (`Order` or `Status`).

  In addition, to correctly load the protocol parameters, you must specify the configuration file for the specific device.

- COS: string in the format `[Object ID]:[Variable ID]`, where:
  - `Object ID` – object identifier represented by an integer.
  - `Variable ID` – variable identifier represented by an integer.

  In addition, to correctly load the protocol parameters, you must specify the configuration file for the station.

- VALMET DNA INTERACTION: string containing the tag name.
- PNU20: integer in the range of 0–65,535.
- GENERAL ELECTRIC EGD: string in the format `[ExchangeId]:[RefAddress]`, where:
  - `ExchangeId` – subscription ID represented by an integer in the range of 0–4,294,967,295.
  - `RefAddress` – tag address offset (in bytes) represented by an integer in the range of 0–65,535.
- KNXnet/IP: integer in the range of 0–65,535.
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS: integer in the range 0–65,535.

An example of the tag address string for the MMS and GOOSE protocols is provided below.

Example:

```
DOMAIN=IED009PROT1;LN=LLN0;CO=DC;DA=NamPlt.configRev;CDC=LPL;LNCDC=LLN0
```

File with descriptions of enumerations: enums.csv

The enumerations description file contains all elements of all enumerations used in the current set of data files for the IEC 61850 standard.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the enums.csv file is provided below.

Example:

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;EnumName;IntValue;TextValue` contains names of columns with data:

- `Connection` – the ID of the connection to which this element belongs.
- `EnumName` – the name of the enumeration.
- `IntValue` – the numerical value of the enumeration.
- `TextValue` – a text description corresponding to the numerical value of enumeration.

The header strings are followed by the file body containing the parameter values (connection ID, name of enumeration, numerical value of enumeration, text description). An example of the enums.csv file is provided below.

Example:

```
'Enums
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;EnumName;IntValue;TextValue
"AA1J1Q01A2";"Beh";1;"on"
"AA1J1Q01A2";"Beh";2;"blocked"
"AA1J1Q01A2";"Beh";3;"test"
"AA1J1Q01A2";"Beh";4;"test/blocked"
"AA1J1Q01A2";"Beh";5;"off"
```

File with descriptions of data sets (tag sets): datasets.csv

The file with descriptions of data sets (tag sets) contains the parameters of data sets for IEC 61850 standard protocols.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the datasets.csv file is provided below.

Example:

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;DatasetName;Deprecated;ItemName` contains the names of columns with data:

- `Connection` – the ID of the connection to which the datasets.csv file belongs.

- `DatasetName` – the name of the data set.

- `Deprecated` – unused data (zero value).

- `ItemName` – full name of the device model element. This can be the final name of a tag or the name of the top branch of the tree.

The header strings are followed by the file body containing the parameter values (connection ID, name of the data set, unused value, and name of the device model element). An example of the datasets.csv file is provided below.

Example:

```
'Datasets
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;DatasetName;Deprecated;ItemName
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDPROT/PTRC1$ST$Tr"
"S7UTDZD";"S7UTDZDPROT/LLN0$DataSet";0;"S7UTDZDMEAS/M1_MMXU1$MX$A$phsA"
```

File with descriptions of MMS protocol reports: iec61850_mms_reports.csv

The file with descriptions of MMS protocol reports contains the parameters for the Reports service of the IEC 61850: MMS protocol.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the iec61850_mms_reports.csv file is provided below.

Example:

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;ReportName;ReportId;DataSetName;IsBuffered` contains the names of columns with data:

- `Connection` – ID of the connection associated with the string of settings in the file iec61850_mms_reports.csv.

- `ReportName` – name of the report.

- `ReportId` – ID of the report.

- `DataSetName` – name of the data set associated with this report.

- `IsBuffered` – indicates whether or not the report is buffered. It takes the `Buffered` or `Unbuffered` value.

The header strings are followed by the file body containing the parameter values (connection ID, report name, report ID, name of the data set for the report, and the buffer indicator). An example of the iec61850_mms_reports.csv file is provided below.

Example:

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

```
"IED24151LD";"IED24151LD/LLN0$BR$brcbST01";"brcbST01";"IED24151LD/LLN0$DSList";"Buffered"
"IED24151LD";"IED24151LD/LLN0$RP$urcbMX01";"urcbMX01";"IED24151LD/LLN0$MXList";"Unbuffered"
```

System event types in Kaspersky Industrial CyberSecurity for Networks

In Kaspersky Industrial CyberSecurity for Networks, events are registered by using the system event types that are automatically created during installation of the application.

Each event type corresponds to a specific event registration technology.

System event types based on Deep Packet Inspection technology

This article provides a description of system event types associated with Deep Packet Inspection technology (see the table below).

System event types based on Deep Packet Inspection technology (DPI)

Code	Title of event type	Registration conditions
4000002900	$technology_rule	Process Control rule was triggered. The following variables are used in the title and description of system event type: • $technology_rule – name of the rule. • $tags – received values of tags whose conditions are defined in the rule. The user-defined settings specified in the triggered Process Control rule are used for the title, description, and scoring of a registered event.
4000000001	Test event (DPI)	A test network packet was detected.

System event types based on Command Control technology

This article provides a description of a system event type associated with Command Control technology (see the table below).

System event type based on Command Control technology (CC)

Code	Title of event type	Registration conditions
4000002602	$systemCommandShort	A monitored system command was detected (and there is no enabled Interaction Control rule for the system command). The following variables are used in the title and description of an event type: • $systemCommandShort – brief description of the detected system command. • $systemCommandFull – detailed description of the detected system command. • $attackTechniques – list of possible techniques from the MITRE ATT&CK Knowledge Base that could be employed by cybercriminals for attacks using this system command.

System event types based on Network Integrity Control technology

This article provides a description of system event types associated with Network Integrity Control technology (see the table below).

System event types based on Network Integrity Control technology (NIC)

Code	Title of event type	Registration conditions
4000002601	Unauthorized network interaction detected ($top_level_protocol)	A network interaction that is not specified in an enabled Interaction Control rule was detected. The following variables are used in the title and description of an event type: • $top_level_protocol – name of the top-level protocol. • $protocol – name of the application-level protocol.
4000002700	No traffic at monitoring point named $monitoringPoint	The network interface linked to the monitoring point has not received traffic in more than 15 seconds. The following variables are used in the title and description of an event type: • $monitoringPoint – name of the monitoring point. • $interface – name of the network interface that is linked to the monitoring point. • $duration – amount of time during which there was no traffic (in seconds).
4000000002	Test event (NIC)	A test network packet was detected (when Network Integrity Control is enabled).

System event types based on Intrusion Detection technology

This article provides a description of system event types associated with Intrusion Detection technology (see the table below).

System event types based on Intrusion Detection (IDS) technology

Code	Title of event type	Registration conditions
4000003000	Rule from the $fileName set (system set of rules) was triggered	Intrusion Detection rule from the system set of rules is triggered. The following variables are used in the title and description of an event type: • $fileName – name of the rule set. • $category – class of the rule. • $ruleName – name of the rule. • $signature_id – rule ID (sid) • $action – type of action to take on network packets defined in the rule (the `drop` or `reject` actions are not performed in Kaspersky Industrial CyberSecurity for Networks).
4000003001	A rule from the $fileName set (user-defined rule set) was triggered.	Intrusion Detection rule from the user-defined rule set is triggered. The following variables are used in the title and description of an event type: • $fileName – name of the rule set. • $category – class of the rule. • $ruleName – name of the rule. • $signature_id – rule ID (sid)

		• $action – type of action to take on network packets defined in the rule (the `drop` or `reject` actions are not performed in Kaspersky Industrial CyberSecurity for Networks).
4000003002	Signs of a brute-force attack or scan were detected	A rule for detecting a scan or brute-force attack was triggered. In the event type description, the $ruleName variable is used for the rule name.
4000004001	Symptoms of ARP spoofing detected in ARP replies	Signs of falsified addresses in ARP packets detected: multiple ARP replies that are not associated with ARP requests. The following variables are used in an event type description: • $senderIp – substituted IP address. • $targetIp – IP address of the target node. • $attackStartTimestamp – time when the first ARP reply was detected.
4000004002	Symptoms of ARP spoofing detected in ARP requests	Signs of falsified addresses in ARP packets detected: multiple ARP requests from the same MAC address to different destinations. The following variables are used in an event type description: • $senderIp – substituted IP address. • $targetIp – IP address of the target node. • $attackStartTimestamp – time when the first ARP reply was detected.
4000005100	IP protocol anomaly detected: data conflict when assembling IP packet	IP protocol anomaly detected: data does not match when overlaying fragments of an IP packet.
4000005101	IP protocol anomaly detected: fragmented IP packet size exceeded	An IP protocol anomaly was detected: the actual total size of a fragmented IP packet after assembly exceeds the acceptable limit.
4000005102	IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	An IP protocol anomaly was detected: the size of the initial fragment of an IP packet is less than the minimum permissible value.
4000005103	IP protocol anomaly detected: mis-associated fragments	An IP protocol anomaly was detected: fragments of an assembled IP packet contain conflicting data on the length of the fragmented packet.
4000002701	TCP protocol anomaly detected: content substitution in overlapping TCP segments	TCP protocol anomaly detected: packets contain overlapping TCP segments with varying contents.
4000000003	Test event (IDS)	A test network packet was detected (with rule-based Intrusion Detection enabled).

System event types based on Asset Management technology

This article provides a description of system event types associated with Asset Management technology (see the table below).

System event types based on Asset Management technology (AM)

Code	Title of event type	Registration conditions
4000005003	Detected new device with the address $owner_ip_or_mac	Asset Management monitoring mode resulted in the automatic addition of a new device based on a detected IP address or MAC address that has not been specified for other devices in the table. When registering the event, the application may simultaneously register the risk named **Unauthorized device** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the device. • $asset_name – assigned name of the device. • $assigned_mac – assigned MAC address (if defined). • $owner_ip – assigned IP address (if defined).

		• $asset_id – ID of the device.
4000005004	Received new information about device with the address $owner_ip_or_mac	Asset Management monitoring mode resulted in the automatic update of device information based on data obtained from traffic. The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the device. • $asset_name – name of the device. • $updated_params – list of updated information. • $asset_id – ID of the device.
4000005005	IP address $owner_ip conflict detected	In Asset Management monitoring mode, the application detected the use of an IP address by a different device than the device for which this IP address was specified. The following variables are used in the title and description of an event type: • $owner_ip – IP address. • $challenger_asset_name – name of the device that used the IP address. • $challenger_mac – MAC address of the device that used the IP address. • $asset_name – name of the device in whose settings the IP address was specified. • $owner_mac – MAC address of the device in whose settings the IP address was specified. • $challenger_ips_list – list of other IP addresses of the device that used the IP address. • $asset_id – ID of the device in whose settings the IP address was specified. • $challenger_id. – ID of the device that used the IP address.
4000005006	Detected traffic from address $owner_ip_or_mac, which is assigned to a device with the Archived status	In Asset Management monitoring mode or based on data received from an EPP application, activity was detected from a device that was assigned the *Archived* status. When registering the event, the application may simultaneously register the risk named **Unauthorized device** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the device. • $asset_name – name of the device. • $last_seen_timestamp – date and time when the device was last seen in the network. • $asset_id – ID of the device.
4000005007	A new IP address $new_ip_addr was detected for the device with MAC address $owner_mac	In Asset Management monitoring mode, a new IP address used by a device was detected. The following variables are used in the title and description of an event type: • $new_ip_addr – detected IP address. • $owner_mac – MAC address of the device. • $asset_name – name of the device. • $owner_ips_list – list of other IP addresses of the device. • $asset_id – ID of the device.
4000005008	MAC address $owner_mac was added to the device with IP address $owner_ip	Asset Management monitoring mode resulted in the automatic addition of a MAC address for a network interface for which only an IP address was specified (the device had the *Unauthorized* or *Archived* status). The following variables are used in the title and description of an event type: • $owner_mac – detected MAC address of the device. • $owner_ip – IP address of the device. • $asset_name – name of the device.

		• $asset_id – ID of the device.
4000005009	IP address $owner_ip was added to the device with MAC address $owner_mac	Asset Management monitoring mode resulted in the automatic addition of an IP address for a network interface for which only a MAC address was specified (the device had the *Unauthorized* or *Archived* status). The following variables are used in the title and description of an event type: • $owner_ip – detected IP address of the device. • $owner_mac – MAC address of the device. • $asset_name – name of the device. • $asset_id – ID of the device.
4000005010	Detected new MAC address $new_mac_addr for device with the IP address $owner_ip	Asset Management monitoring mode resulted in the detection of a new MAC address used by a device (auto update of address information is disabled for the device). The following variables are used in the title and description of an event type: • $new_mac_addr – detected MAC address. • $owner_ip – IP address of the device. • $asset_name – name of the device. • $asset_id – ID of the device.
4000005011	Change of MAC address $owner_mac to $challenger_mac detected in device information received from EPP application	The MAC address of a device was updated according to data received from an EPP application. The following variables are used in the title and description of an event type: • $owner_mac – old MAC address of the device. • $challenger_mac – new MAC address of the device. • $asset_name – name of the device. • $asset_id – ID of the device.
4000005012	New address information for device $asset_name found in data received from EPP program	New address information of a device was detected in data received from an EPP application. This type of event is registered if a change in device address information was not processed by the application as an event with code 4000005009 or 4000005010. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $unaccepted_epp_addresses – address information. • $asset_id – ID of the device.
4000005013	Conflict detected in addresses of devices $conflicted_epp_assets after data received from EPP program	Based on data received from an EPP application, a conflict was detected in the addresses of multiple devices in Kaspersky Industrial CyberSecurity for Networks. According to data from the EPP application, the addresses belong to the same device. The following variables are used in the title and description of an event type: • $conflicted_epp_assets – devices with conflicting addresses detected. • $unaccepted_epp_addresses – addresses that belong to the same device.
4000005014	Subnet $subnet_mask added based on data from EPP application	After data was received from an EPP application, a new subnet was automatically added to the list of known subnets. The subnet is added to an address space in which the data source may be the integration server that received data from an EPP application. If there are several of these address spaces available, the application chooses the address space that contains the most suitable subnet for automatically adding a new nested subnet. The following variables are used in the title and description of an event type: • $subnet_mask – subnet address. • $subnet_type – subnet type.
4000005015	Equipment change is detected for the device	Based on the data received from the EPP application, the device equipment information was updated using the equipment monitoring functionality.

	with the following address: $owner_ip_or_mac	The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the device. • $asset_name – name of the device. • $asset_id – ID of the device. • $ added_asset_hardware – list of added equipment. • $ modified_asset_hardware – list of modified equipment. • $ removed_asset_hardware – list of removed equipment.
4000005200	PLC Project Control: detected read of unknown block from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of an unknown block of a project from a PLC (if there is no saved information about this block). When registering the event, the application may simultaneously register the risk named **Reading unknown block of project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name – name of the block. • $saved_date_time – date and time when the operation was detected.
4000005201	PLC Project Control: detected read of known block from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of a known block of a project from a PLC (if there is saved information about this block but the received information does not match the latest saved information about this block). When registering the event, the application may simultaneously register the risk named **Reading known block of project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name – name of the block. • $saved_date_time – date and time when the block was saved in the application.
4000005202	PLC Project Control: detected write of new block to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of an unknown block of a project from a PLC (if there is no saved information about this block). When registering the event, the application may simultaneously register the risk named **Writing new block of project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name – name of the block. • $saved_date_time – date and time when the operation was detected.
4000005203	PLC Project Control: detected write of known block to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a known block of a project from a PLC (if there is saved information about this block but the received information does not match the latest saved information about this block). When registering the event, the application may simultaneously register the risk named **Writing known block of project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name – name of the block. • $saved_date_time – date and time when the block was saved in the application.
4000005204	PLC Project Control: detected read of unknown project from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of an unknown project from a PLC (if there is no saved information about this project). When registering the event, the application may simultaneously register the risk named **Reading unknown project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type:

		- $asset_name – name of the device. - $saved_date_time – date and time when the operation was detected.
4000005205	PLC Project Control: detected read of known project from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of a known project from a PLC (if there is saved information about this project but the received information does not match the latest saved information about this project). When registering the event, the application may simultaneously register the risk named **Reading known project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: - $asset_name – name of the device. - $saved_date_time – date and time when the project was saved in the application.
4000005206	PLC Project Control: detected write of new project to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a new project to a PLC (if there is no saved information about this project). When registering the event, the application may simultaneously register the risk named **Writing new project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: - $asset_name – name of the device. - $saved_date_time – date and time when the operation was detected.
4000005207	PLC Project Control: detected write of known project to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a known project to a PLC (if there is saved information about this project but the received information does not match the latest saved information about this project). When registering the event, the application may simultaneously register the risk named **Writing known project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: - $asset_name – name of the device. - $saved_date_time – date and time when the project was saved in the application.
4000000004	Test event (AM)	A test network packet was detected (with the device activity detection method enabled).

System event types based on External technology

This article provides a description of system event types associated with External technology (see the table below).

System event types based on External technology (EXT)

Code	Title of event type	Registration conditions
8000000001	Incident	A sequence of events satisfying the conditions of a correlation rule was detected. When an event is registered, the incident receives a title and description from the correlation rule.
4000005400	Event from an external system	An event was received from an external system using the Kaspersky Industrial CyberSecurity for Networks API. When an event is registered, the contents of the title and description are determined by the external system.

System event types based on Endpoint Protection Platform

This article provides a description of system event types associated with Endpoint Protection Platform technology (see the table below).

System event type based on Endpoint Protection Platform (EPP)

Code	Title of event type	Registration conditions
4000005500	Activity specific for network attacks	The integration server received data indicating that the Network Threat Protection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005501	Connection of an untrusted external device	The integration server received data indicating that the Device Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005502	Attempt to run an unauthorized or untrusted application	The integration server received data indicating that the Application Launch Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005503	Prohibited file operation in the specified monitoring scope	The integration server received data indicating that the File Integrity Monitor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005504	Files in the specified monitoring scope are modified	The integration server received data indicating that the Baseline File Integrity Monitor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005505	Network connection not allowed by firewall rules	The integration server received data indicating that the Firewall Management component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005506	System registry modifications in the specified monitoring scope	The integration server received data indicating that the Registry Access Monitor component of the EPP application is triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005507	Log analysis rule is triggered	The integration server received data indicating that a rule of the Log Inspection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005508	Attempt to exploit a vulnerability in a protected process	The integration server received data indicating that the Exploit Prevention component of the EPP application is triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005509	Attempt to maliciously encrypt network file resources	The integration server received data indicating that the Anti-Cryptor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005510	Attempt to connect to a Wi-Fi network	The integration server received data indicating that the Wi-Fi Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005511	PLC project was modified compared to the baseline	The integration server received data indicating that the PLC Project Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005512	Infected or probably infected object is detected	The integration server received data indicating that the Real-Time File Protection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.

Categories of system commands in Kaspersky Industrial CyberSecurity for Networks

This article lists the categories of system commands supported by Kaspersky Industrial CyberSecurity for Networks when analyzing industrial network traffic (see the table below).

Categories of system commands

Category of system commands	Description
`Connection`	Connection management commands.
`Authentication`	Authentication commands.
`Operating mode changes`	Commands for changing the operating mode of devices.
`Download program`	Commands for downloading a program of devices.
`Upload program`	Commands for uploading a program of devices.
`Control commands`	Standardized commands for protocols of intelligent electronic devices (IED).
`Modify program`	Commands for changing the control program of a device.
`Alarm signal management`	Commands for managing alarm signals.
`Online mode`	Commands for working with a program of devices in online mode or debug mode.
`Modify tags`	Commands for enforcing modifications to tag values.
`Reading tags and data`	Commands for receiving tag values, subscribing to tags, and requesting data on programs of devices.
`Update firmware`	Commands for modifying the firmware of devices.
`Read device configuration`	Commands for reading or requesting device information.
`Change device configuration`	Commands for modifying the settings of devices.
`File operation`	Commands for managing files and directories of devices.
`Service command`	Commands for servicing devices.
`Date and time management`	Commands for managing the date and time on devices.
`Diagnostic message`	Diagnostic messages regarding errors or mismatched data in traffic.
`Interaction via DCOM`	Commands of protocols that use DCOM technology (for example, OPC DA).
`Message parsing error`	Errors when parsing messages.
`Other`	Commands not assigned to other specific categories.

Examples of using address spaces in Kaspersky Industrial CyberSecurity for Networks

Address spaces (AS) enable operation of Kaspersky Industrial CyberSecurity for Networks in situations in which devices with identical addresses are used in different network segments. This article provides examples of using address spaces for the following options when duplicating device addresses in different network segments:

- Duplication of IP addresses
- Duplication of MAC addresses
- Duplication of MAC addresses and use of identical ranges of IP addresses

Address spaces for duplicating IP addresses of devices

This example examines a company that has 16 industrial sites with groups of PLCs at these sites. Each industrial site uses the same ranges of IP addresses: 10.4.0.0/16, 10.5.0.0/16, 10.8.0.0/16, 10.9.0.0/16. This means that devices at different sites may have identical IP addresses.

The network segments of industrial sites are completely isolated from the main enterprise network. Each segment contains operational PLCs, engineering workstations, and computers performing functions of application stations (hereinafter referred to as "Application Station" computers). A segment is integrated with the main enterprise network through an Application Station computer. This computer has a dedicated network interface with a unique IP address on the main enterprise network.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, the following objects must be added for each industrial site segment:

- Monitoring point for receiving traffic within the segment
- Monitoring point for receiving traffic from the Application Station computer
- Address space containing one rule

For example, you can add objects with the following names for the first segment:

- **MPoint_1-1**
- **MPoint_1-2**
- **Site_1**

The settings of address spaces for each segment are described in the table below.

AS for segments with identical IP addressing

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points:** MPoint_1-1 MPoint_1-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_2	**Monitoring points:** MPoint_2-1 MPoint_2-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_3	**Monitoring points:** MPoint_3-1 MPoint_3-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
...				
Site_16	**Monitoring points:** MPoint_16-1 MPoint_16-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16

Address spaces for duplicating MAC addresses of devices

This example examines an industrial network that uses VLAN technology. The network has two dedicated segments for industrial sites distinguished by the IDs VLAN 3910 and 3915. The network segments contain devices with manually assigned MAC addresses (the devices and their software support this capability). This means that devices in different network segments may have identical MAC addresses.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, an address space must be added for each segment. For example, the names **Site_1** and **Site_2** can be assigned to the address spaces. Address spaces may contain one rule each.

The settings of address spaces for each segment are described in the table below.

AS for segments with identical MAC addressing

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points: any**	**Data Link (L2)**	3910	**Any**
Site_2	**Monitoring points: any**	**Data Link (L2)**	3915	**Any**

Address spaces for duplicating MAC addresses of devices with the same range of IP addresses

This example examines an industrial network that uses VLAN technology. The network has two dedicated segments for industrial sites distinguished by the IDs VLAN 3910 and 3915. The network segments contain devices with manually assigned MAC addresses (the devices and their software support this capability). The IP addresses in each segment are in the same addresses range: 140.80.0.0/16. This means that devices in different network segments may have identical MAC addresses and/or identical IP addresses.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, an address space must be added for each segment. For example, the names **Site_1** and **Site_2** can be assigned to the address spaces. Address spaces may contain one rule each.

The settings of address spaces for each segment are described in the table below.

AS for segments with identical MAC addressing and identical IP address ranges

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points: any**	**Data Link and Network (L2 and L3)**	3910	140.80.0.0/16
Site_2	**Monitoring points: any**	**Data Link and Network (L2 and L3)**	3915	140.80.0.0/16

Supported common protocols

Kaspersky Industrial CyberSecurity for Networks supports monitoring of the following common protocols in traffic:

- Bitcoin
- Bittorrent
- BOOTP / DHCP
- DNS

- FTP
- GLBP
- HTTP
- HTTPS
- ICMP
- IMAP
- IRC
- Jabber®
- Litecoin
- MQTT
- NBNS
- NetBIOS
- NTP
- POP3
- Radius
- Radmin
- RDP
- RLOGIN
- SIP
- SMB
- SMTP
- SNMP
- SSDP
- SSH
- SSL / TLS
- Syslog
- Telegram
- Telnet

- TFTP
- TNS
- Tor®
- VNC
- VRRP

Device operating systems supported to perform active polling of devices

This article lists the device operating systems supported by the application for active polling of devices.

Windows operating systems

Kaspersky Industrial CyberSecurity for Networks supports active devices with the following versions of Windows:

- Desktop operating systems:
  - Windows 2000 SP4 and later
  - Windows XP Professional SP2 and later x86 versions
  - Windows Vista® SP 2 x86/x64
  - Windows 7 Family:
    - Windows 7 Enterprise x86/x64
    - Windows 7 Professional x86/x64
    - Windows 7 Ultimate x86/x64
    - Windows 7 Enterprise SP1 and later x86/x64
    - Windows 7 Professional SP1 and later x86/x64
    - Windows 7 Ultimate SP1 and later x86/x64
  - Windows 8 Enterprise x86/x64
  - Windows 8 Pro x86/x64
  - Windows 8.1 Enterprise x86/x64
  - Windows 8.1 Pro x86/x64
  - Windows 10 Family:
    - Windows 10 Pro x86/x64

    - Windows 10 Enterprise LTSC 2015 x86/x64
    - Windows 10 Enterprise LTSC 2016 x86/x64
    - Windows 10 Enterprise LTSC 2019 x86/x64
    - Windows 10 version 1507
    - Windows 10 version 19H1
    - Windows 10 version 20H1
    - Windows 10 version 21H1
    - Windows 10 version 1607
    - Windows 10 version 1703
    - Windows 10 version 1709
    - Windows 10 version 1803
    - Windows 10 version 1809
- Server operating systems:
  - Windows Server® 2003 Enterprise SP1 and later x86/x64
  - Windows Server 2003 Standard SP1 and later x86/x64
  - Windows Server 2008 Enterprise SP2 and later
  - Windows Server 2008 Standard SP2 and later
  - Windows Server 2008 R2 Enterprise SP1 and later
  - Windows Server 2008 R2 Standard SP1 and later
  - Windows 2012 Family:
    - Windows Server 2012 Datacenter x64
    - Windows Server 2012 Essentials x64
    - Windows Server 2012 Foundation x64
    - Windows Server 2012 Standard x64
    - Windows Server 2012 R2 Datacenter x64
    - Windows Server 2012 R2 Essentials x64
    - Windows Server 2012 R2 Foundation x64
    - Windows Server 2012 R2 Standard x64

  - Windows Server 2016 Datacenter x64
  - Windows Server 2016 Essentials x64
  - Windows Server 2016 Standard x64
  - Windows Server 2019 Datacenter x64
  - Windows Server 2019 Essentials x64
  - Windows Server 2019 Standard x64
- Embedded operating systems:
  - Windows XP Embedded SP3 x86 (POS Ready 2009)
  - Windows Embedded 7 SP1 x86/x64 (POS Ready 7)
  - Windows Embedded 8.0 Standard x86/x64
  - Windows Embedded 8.1 Industry Pro x86/x64
  - Windows 10 IoT family:
    - Windows 10 IoT Enterprise 19H1
    - Windows 10 IoT Enterprise 20H1
    - Windows 10 IoT Enterprise 21H1
    - Windows 10 IoT Enterprise, version 1607
    - Windows 10 IoT Enterprise, version 1703
    - Windows 10 IoT Enterprise, version 1709
    - Windows 10 IoT Enterprise, version 1803
    - Windows 10 IoT Enterprise, version 1809
    - Windows 10 IoT Enterprise version 1507 (10240.18818) x86/x64

Linux operating systems

Kaspersky Industrial CyberSecurity for Networks supports active devices with the following versions of Linux:

- 32-bit operating systems:
  - CentOS 6.7 and later
  - Debian GNU / Linux 9.4 and later
  - Debian GNU / Linux 10.1 and later
  - Linux Mint 19 and later

  - Red Hat® Enterprise Linux 6.7 and later
- 64-bit operating systems:
  - Astra Linux Common Edition (regular update 2.12)
  - Astra Linux Special Edition RUSB.10015-01 (regular update 1.5)
  - Astra Linux Special Edition RUSB.10015-01 (regular update 1.6)
  - Astra Linux Special Edition RUSB.10015-16 (version 1) (regular update 1.6)
  - CentOS 6.7 and later
  - CentOS 7.2 and later
  - CentOS 8.0 and later
  - Debian GNU / Linux 9.4 and later
  - Debian GNU / Linux 10.1 and later
  - Linux Mint 19 and later
  - Linux Mint 20.1 and later
  - openSUSE Leap 15.0 and later
  - Oracle® Linux 7.3 and later
  - Oracle Linux 8.0 and later
  - Red Hat Enterprise Linux 6.7 and later
  - Red Hat Enterprise Linux 7.2 and later
  - Red Hat Enterprise Linux 8.0 and later
  - SUSE Linux Enterprise Server 15 and later
  - Ubuntu 18.04 LTS and later
  - Ubuntu 20.04 LTS

Detecting attributes and typical device interactions in Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks can detect important information about the infrastructure in the network traffic by passive analysis of the device activities in the industrial network and save information about the detected network devices, their attributes, and interactions.

To ensure that Kaspersky Industrial CyberSecurity for Networks can obtain the most accurate and complete information about the process control system components, their attributes, and typical network interactions, it is recommended to perform various maintenance and routine operations in the control system. These can be any operations considered acceptable. The operations must be safe and must not interrupt or impact the normal technological process by other means.

These operations may include but are not limited to:

- Network device polling.
- Initiating the operations between SCADA servers, Historian, HMI, and PLC.
- Connecting to PLCs and IEDs using the appropriate engineering software.
- Uploading and downloading PLC projects.
- Requesting information about the PLC configurations and firmware versions.
- Rebooting SCADA servers, Historian, operator and engineer workstations.
- Restarting PLCs and / or IEDs.

For instructions on how to perform operations, see the software and hardware documentation for your process control system.

Configuring port mirroring for Kaspersky Industrial CyberSecurity for Networks

For correct operation, Kaspersky Industrial CyberSecurity for Networks must receive a copy of network traffic sent from the industrial network switch configured to transmit mirrored network packets to the assigned network port. This technology of network traffic mirroring is called Switched Port Analyzer (SPAN) or Port Mirroring.

Below are port mirroring configuration examples for some Ethernet switch models, which can be used in the industrial network infrastructure:

- Cisco™ Access and Distribution Switches

You can configure a SPAN session for Cisco Access and Distribution switches (for example, Cisco Catalyst™ 2960 and Cisco Catalyst 3850) using the switch command line interface. To do this, access the target switch via Ethernet or console port and open the switch management functions. In configuration mode, create a new monitoring session, select a range of source interfaces to mirror and analyze traffic, set the destination interface and save the configuration.

For more information about configuring port mirroring for Cisco Access and Distribution switches, refer to Cisco hardware documentation.

To configure port mirroring for Cisco Access and Distribution switches:

1. From the privileged EXEC mode, enter the global configuration mode using the following command:

   ```
   conf t /
   ```

2. To view the existing monitor sessions, enter the following command:

   ```
   show monitor session all /
   ```

3. If necessary, delete the existing monitor session:

   ```
   no monitor session <session number> /
   ```

   where `<session number>` is the number of the monitor session to be deleted. You can specify a value from 1 to 66. You can use the following keywords instead of the session number:

   - `all` – to delete all monitor sessions
   - `local` – to delete local monitor sessions
   - `remote` – to delete remote monitoring sessions

4. Specify the source port numbers:

   ```
   monitor session <session number> source interface <source port>/<VLAN ID> -
   <source port>/<VLAN ID> /
   ```

   where:

   - `<session number>` – monitor session number
   - `<source port>` – source port number
   - `<VLAN ID>` – VLAN identifier

5. Specify the destination port numbers:

   ```
   monitor session <session number> destination interface <destination port> / <destination
   port> encapsulation replicate /
   ```

   where:

   - `<session number>` – monitor session number
   - `< destination port>` – number of the destination port

6. Return to the privileged EXEC mode using the following command:

   ```
   end /
   ```

7. To check the monitor session configuration, enter the following command:

```
show monitor /
```

8. To activate SPAN settings after rebooting the switch, save the monitor session configuration to a configuration file:

   ```
   copy running-config startup-config /
   ```

- Cisco Small Business™ switches

  For more information on configuring Cisco Small Business switches, refer to Cisco documentation.

  To configure port mirroring for Cisco Small Business switches:

  1. Connect to the switch and open port mirroring settings in the switch web interface.
  2. Select **Administration** → **Diagnostics** → **Port and VLAN mirroring** section.
  3. Add source interfaces and select the destination interface.
  4. Save the changes.

- Hirschmann Industrial Ethernet Switches

  For more information about configuring port mirroring for Hirschmann Industrial Ethernet switches, refer to Hirschmann hardware documentation.

  To configure port mirroring for Hirschmann Industrial Ethernet switches:

  1. Connect to the switch.
  2. In the switch web interface , select **Diagnostics** → **Port Mirroring**.
  3. As a source, select all the necessary RX and TX ports for ingress and egress monitoring.
  4. Select the destination port to be connected to Kaspersky Industrial CyberSecurity for Networks device.
  5. To enable mirroring, select **On** in the **Operation** section, and then select **Set**.

     Changes will be applied to the volatile memory (RAM) of the device.
  6. To save the changes permanently, open the dialog window and click **Save**.

- Siemens SCALANCE Switches

For more information about configuring port mirroring for Siemens SCALANCE switches, refer to Siemens hardware documentation.

To configure port mirroring for Siemens SCALANCE switches:

1. Connect to the switch web interface and select **Layer 2** → **Mirroring**.
2. To create a mirroring session:
   1. Select the **General** tab.
   2. Enable Mirroring.
   3. To create a record in the table, click the **Create** button.

      The session ID is assigned automatically.
   4. In the **Session Type** drop-down list, select the **Port Based** value.
   5. Click the **Set Values** button.
   6. In the **Destination Port** column, select the destination port.

      For example, **P0.8**.
   7. Click the **Set Values** button.
3. Select the **Port** tab.
4. In the **Port** tab follow these steps:
   1. In the **Session ID** drop-down list, select the ID of the session you created earlier in the **General** tab.
   2. To monitor all data traffic of a port, select all the ports in the table in the **Ingress** and **Egress** columns.
   3. Click the **Set Values** button.

- Siemens RUGGEDCOM i800, i801, i802, i803 Switches ?

For more information about configuring port mirroring for Siemens RUGGEDCOM switches, refer to Siemens hardware documentation.

To configure port mirroring for Siemens RUGGEDCOM i800, i801, i802, i803 switches:

1. Connect to the switch web interface.

   Default connection to the device is established via IP address 192.168.0.1/24.

2. Select **Ethernet Ports** → **Configure Port Mirroring**.

3. For the **Port Mirroring** setting, select **Enabled**.

4. Specify the source port number in the **Source Port** setting.

5. For the **Source Direction** setting, select **Egress and Ingress**.

6. Specify the destination port number in the **Target Port** setting.

7. Click the **Apply** button.

You can get similar information about configuring other models of switches in the documentation for your network equipment.

Glossary

Account role

Set of access rights that determine the actions available to a user when connected to the Server through the web interface. Kaspersky Industrial CyberSecurity for Networks provides the Administrator role and the Operator role.

Address space (AS)

A network segment defined by the rules that determine sets of addresses, VLAN identifiers, or monitoring points.

ARP spoofing

A technique used by criminals to conduct a "man-in-the-middle" attack on networks that use ARP (Address Resolution Protocol).

Asset Management

Technology for registering events associated with the detection of device information in traffic or in data received from EPP applications (for example, an event for the detection of activity from a previously unknown device).

Command Control

Technology for registering events associated with the detection of system commands for devices in traffic (for example, detection of an unauthorized system command).

CVE

Acronym for Common Vulnerabilities and Exposures. Database of publicly known vulnerabilities and information security risks. Vulnerabilities described in this database are assigned identification numbers in the format CVE-<year>-<number>.

Dedicated Kaspersky Industrial CyberSecurity network

A computer network consisting of computers designed for running applications that are part of the Kaspersky Industrial CyberSecurity solution, and the network equipment that enables interaction between computers. The dedicated network must not be accessible from other networks.

Deep Packet Inspection

Technology for registering events associated with process violations (for example, the set temperature value has been exceeded).

Device

Device that is connected to a computer network and is identified by address information that can be saved in Kaspersky Industrial CyberSecurity for Networks (for example, programmable logic controller, remote terminal, or intelligent electronic device).

Device vulnerability

A defect in device hardware or software that can be exploited by a hacker to impact the operation of the information system or to gain unauthorized access to information.

Endpoint Protection Platform (EPP)

An integrated system providing comprehensive Endpoint Protection (such as mobile devices, computers or laptops) by using various security technologies. An example of an Endpoint Protection Platform is the solution known as Kaspersky Endpoint Security for Business.

EPP application

An application that is included in the Endpoint Protection Platform (EPP). EPP applications are installed to endpoint devices within an enterprise IT infrastructure (such as mobile devices, computers or laptops). One example of an EPP application is Kaspersky Endpoint Security for Windows included in the EPP solution known as Kaspersky Endpoint Security for Business.

Event

Record containing information requiring the attention of an ICS security officer. Kaspersky Industrial CyberSecurity for Networks saves registered events in the database. To view registered events, you need to connect to the Server through the web interface. If necessary, you can configure transmission of events to Kaspersky Security Center and recipient systems.

Event correlation rule

Set of conditions for checking sequences of events in Kaspersky Industrial CyberSecurity for Networks. When Kaspersky Industrial CyberSecurity for Networks detects a sequence of events that meet the conditions of an event correlation rule, the application registers an incident.

Event type

Defined set of parameters for registering events in Kaspersky Industrial CyberSecurity for Networks. A unique number (event type code) is assigned to each event type.

External

Technology for registering incidents and events that are received by Kaspersky Industrial CyberSecurity for Networks from recipient systems using Kaspersky Industrial CyberSecurity for Networks API methods.

ICS

Abbreviation for Industrial Control System. A package of hardware and software designed to automate control of process equipment at industrial enterprises.

Incident

In Kaspersky Industrial CyberSecurity for Networks, an incident is an event that is registered when a specific sequence of events is received. Incidents group events that have certain common traits or that are associated with the same process. Kaspersky Industrial CyberSecurity for Networks registers incidents based on event correlation rules.

Industrial network

Computing network that links the nodes of an automated Industrial Control System of an industrial enterprise.

Intelligent electronic device (IED)

A set of devices that ensure timely disconnection of faulty power facilities from the power system, and that perform the necessary actions to ensure normal operation of the power system in automated or semi-automated operating modes.

Interaction Control rule

A description of authorized communications for industrial network devices. When Kaspersky Industrial CyberSecurity for Networks detects network interaction that satisfies an enabled Interaction Control rule, the application does not register an event.

Intrusion Detection

Technology for registering events associated with the detection of traffic anomalies that are signs of an attack (for example, detection of signs of ARP spoofing).

Intrusion Detection rule

A set of conditions used by the Intrusion Detection system to analyze traffic. The rule describes a traffic anomaly that could be a sign of an attack in the industrial network.

IOC

Indicator of Compromise. A set of data on a malicious object or action.

IOC file

File containing a set of IOC indicators that, if matched, the application considers an event to be a detection. The likelihood of detection may increase if the check identifies exact matches of the object data with multiple IOC files.

Kaspersky Industrial CyberSecurity for Networks Sensor

Kaspersky Industrial CyberSecurity for Networks component. A sensor is installed on a separate computer (not on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server). A sensor receives and analyzes data from computer networks that are connected to the network interfaces of the sensor's computer. To receive and analyze industrial network traffic, monitoring points must be added to the network interfaces. A sensor forwards the data analysis results to the Server.

Kaspersky Industrial CyberSecurity for Networks Server

Kaspersky Industrial CyberSecurity for Networks component. The Server receives data, processes it, and provides it to users of the application. The Server can receive data from sensors or independently obtain and analyze data from computer networks that are connected to the network interfaces of the Server computer.

Link on the network map

Object on the network map represented by a line linking the nodes. On the network interactions map, shows the interaction of nodes. On the topology map, shows the physical connection of nodes.

Manageable connector

A software module for data exchange with the application; it provides automatic registration, startup, and control capabilities. Only nodes that have application components installed can serve as deployment nodes for manageable connectors.

Monitoring point

A point where incoming data is received. It is added to the network interface of a node hosting the Server or sensor of Kaspersky Industrial CyberSecurity for Networks, and is used for receiving a copy of industrial network traffic (for example, from a network switch port configured to transmit mirrored traffic).

Network Integrity Control

Technology for registering events associated with industrial network integrity or the security of communications (for example, detection of communication between devices over an unauthorized protocol).

Network interactions map

Model that visually represents detected communications between devices. The network interactions map contains the following objects: nodes corresponding to devices, device groups, and links between nodes/device groups.

Node

Computer on which a Kaspersky Industrial CyberSecurity for Networks Server or sensor is installed, or an object on the network map representing one or multiple devices.

PLC project

Microprogram written for a PLC. It is stored in PLC memory and is run as part of the industrial process that uses the PLC. A PLC project may consist of blocks that are individually transmitted and received over the network when the project is read or written.

Process Control rule

A set of conditions for tag values. When the conditions of a Process Control rule are fulfilled, Kaspersky Industrial CyberSecurity for Networks registers an event.

Programmable Logic Controller (PLC)

Industrial controller used to automate enterprise processes.

Risk

A potential threat to the information system resources detected when analyzing traffic and device information.

SCADA

Abbreviation for Supervisory Control And Data Acquisition. A software suite that enables the operator to control industrial processes in real time.

Security policy

Set of data that determines the operational settings of Kaspersky Industrial CyberSecurity for Networks.

SIEM

Abbreviation for Security Information and Event Management. This is a solution for managing information and events in an organization's security system.

Single Sign-On (SSO) technology

Mechanism that allows a user to access multiple software resources using the same user account.

System command

Data block in industrial network traffic containing a control command (for example, START PLC) or a system message related to device operation or containing packet analysis results (for example, REQUEST NOT FOUND).

Tag

Variable that contains the value of a specific process parameter such as temperature.

Topology Map

A model for visual representation of the scheme of physical connections between devices in the industrial network. The topology map contains the following objects: nodes representing devices and network equipment, and links representing physical connections of the nodes.

Unmanaged connector

Manually controlled software module for data exchange with the application.

Unmanaged switch

A device without address information for which connections on the topology map are detected or are potentially available.

Information about third-party code

Information about third-party code is contained in the file named legal_notices.txt in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Flash are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

BACnet is a registered trademark of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

iPad, iPhone, Mac, Mac OS, macOS, and OS X are trademarks of Apple Inc.

AXIS and AXIS COMMUNICATIONS are registered trademarks or trademark applications of Axis AB in various jurisdictions.

BitTorrent is a trademark of BitTorrent, Inc.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu and LTS are registered trademarks of Canonical Ltd.

Cisco, Cisco AnyConnect, Cisco Catalyst, Cisco Small Business, AnyConnect, IOS, Jabber, and Snort are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Dropbox is a trademark of Dropbox, Inc.

Radmin is a registered trademark of Famatech.

Fortinet, FortiGate, and FortiOS are either registered trademarks or trademarks of Fortinet Corporation in the United States and/or other countries.

FreeBSD is a registered trademark of The FreeBSD Foundation.

General Electric and Multilin are registered trademarks of General Electric Company.

Google, Android, Chrome, Chromium, Google Chrome, and Nexus are trademarks of Google LLC.

HL7 is a registered trademark of Health Level Seven International and its use does not constitute endorsement by HL7.

Hitachi is a trademark of Hitachi, Ltd.

Intel, Atom, Core, and Itanium are trademarks of Intel Corporation in the United States and/or other countries.

IBM and DB2 are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Node.js is a trademark of Joyent, Inc.

Juniper is a trademark or registered trademark of Juniper Networks, Inc. in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

Microsoft, Active Directory, ActiveX, AppLocker, BitLocker, BizTalk, Cortana, Internet Explorer, Microsoft Edge, Outlook, PowerShell, SmartScreen, SpyNet, SQL Server, Visual Basic, Visual FoxPro, Win32, Windows, Windows PowerShell, Windows Server, Windows Store, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

CVE is a registered trademark of The MITRE Corporation.

CWE, CWSS, CWRAF, and the CWE logo are trademarks of The MITRE Corporation.

OVAL and the OVAL logo are registered trademarks of The MITRE Corporation.

MOXA is a registered trademark of Moxa Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the United States and other countries.

DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

ONVIF is a trademark of ONVIF, Inc.

OpenVPN is a registered trademark of OpenVPN, Inc.

Oracle, Java, JavaScript, and Solaris are registered trademarks of Oracle and/or its affiliates.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, Ansible, CentOS, and Fedora are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Remote Utilities is a registered trademark of Remote Utilities LLC in the United States and/or other countries.

The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

Schneider Electric is a trademark of Schneider Electric.

Sendmail and other names and product names are trademarks or registered trademarks of Sendmail, Inc.

Siemens, Simatic, and WinCC are registered trademarks of Siemens AG.

OpenWRT is a trademark of Software Freedom Conservancy (SFC). Kaspersky Industrial CyberSecurity for Networks is not affiliated with OpenWrt.

Debian is a registered trademark of Software in the Public Interest, Inc.

Dameware is trademark of SolarWinds Worldwide, LLC, registered in the United States and other countries.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

VxWorks is a registered trademark (®) or service mark (SM) of Wind River Systems, Inc. This product is not affiliated with, endorsed, sponsored, supported by the owners of the third-party trademark mentioned herein.