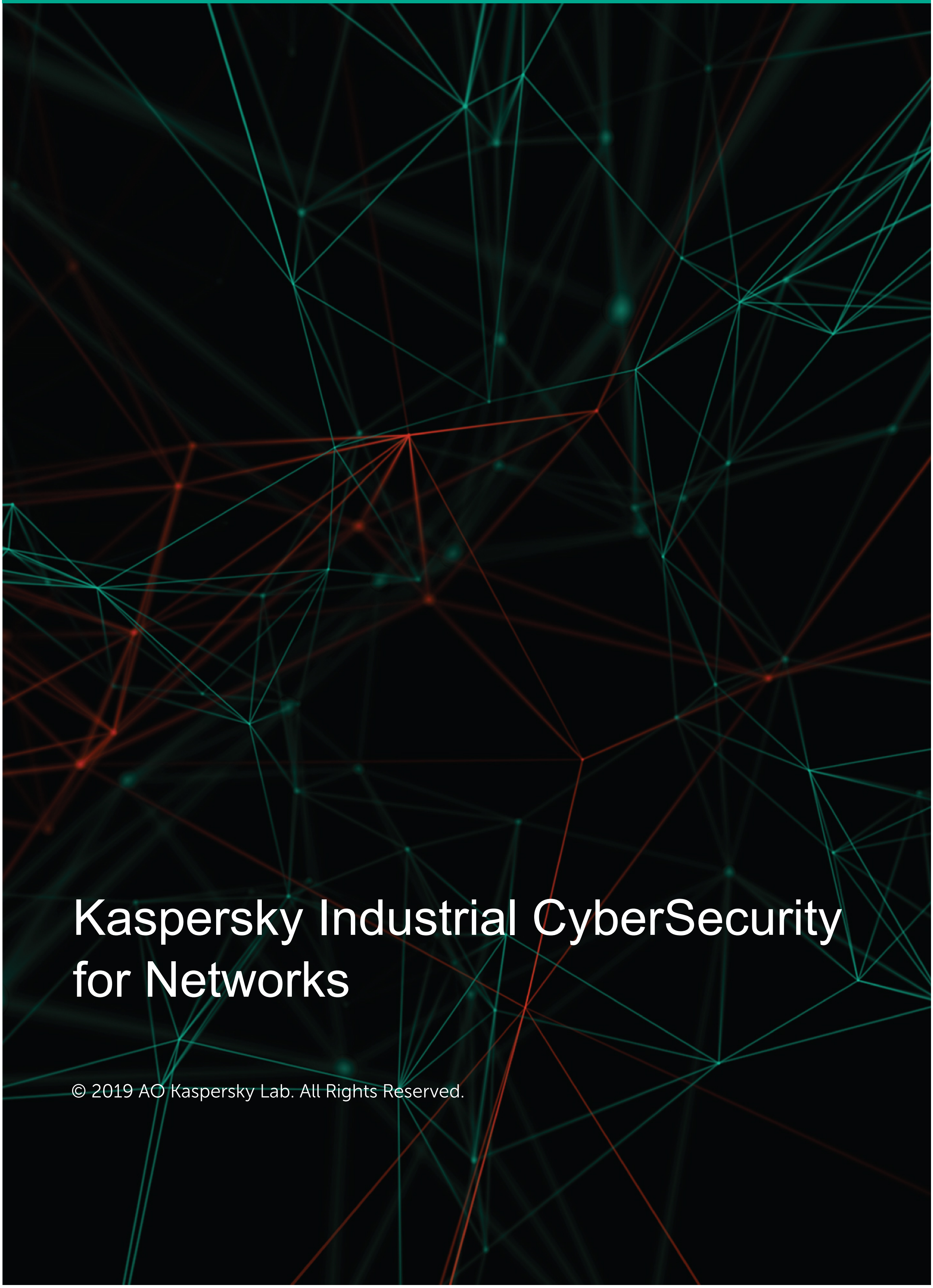


Kaspersky Industrial CyberSecurity for Networks

Contents

- About Kaspersky Industrial CyberSecurity for Networks
  - Distribution kit
  - Hardware and software requirements
  - Overview of Kaspersky Industrial CyberSecurity for Networks functionality
  - Security recommendations for Kaspersky Industrial CyberSecurity for Networks
- What's new
- Application architecture
- Installing and removing the application
  - Common deployment scenarios
  - Preparing for application installation
  - Installation menu commands
    - Installation menu commands for Server management
    - Installation menu commands for sensor management
    - General installation menu commands
    - Installation menu exit commands
  - Application installation procedure
  - Viewing the End User License Agreement and Privacy Policy
  - Reconfiguring and reinstalling the application
  - Installing the application in non-interactive mode
  - Reinforcing the security of computers with application components installed
  - Installing the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center
  - Getting started
  - Upgrading from a previous version of the application
  - Removing the application
- Starting and stopping the application
  - Connecting to the Server through a web browser
  - Closing a Server connection session through a web browser
  - Starting the Application Console
  - Closing the application Console
- Application interface
  - Web interface of Kaspersky Industrial CyberSecurity for Networks
    - Page for entering account credentials to connect through a web browser
    - Menu of the Kaspersky Industrial CyberSecurity for Networks web interface
    - Dashboard section
    - Assets section
    - Network map section
    - Events section
    - Tags section
    - Network Control section
    - Settings section
  - Kaspersky Industrial CyberSecurity for Networks Console
    - Elements of the Kaspersky Industrial CyberSecurity for Networks Console interface
    - Process control tab
    - Configure events tab
    - Intrusion detection tab
    - Settings of Server and sensors window

Manage logs window

Manage updates window

Update license key window

Licensing the application

About the End User License Agreement

About the Privacy Policy

About the license

About the license certificate

About the license key used for activating update functionality

About the license key file used for activating update functionality

Adding a license key in the Application Console

Viewing information about an added license key in the Application Console

Removing a license key in the Application Console

Processing and storing data in Kaspersky Industrial CyberSecurity for Networks

About data provision

About logs

Folders for storing application data

Administration of Kaspersky Industrial CyberSecurity for Networks

Managing monitoring points

Adding a monitoring point

Enabling monitoring points

Disabling monitoring points

Renaming a monitoring point

Deleting a monitoring point

Identifying the Ethernet port associated with a network interface

Monitoring the state of Kaspersky Industrial CyberSecurity for Networks

Monitoring the application state when connected through the web interface

Viewing application messages

Viewing user activity audit entries

Monitoring the application state in the Kaspersky Industrial CyberSecurity for Networks Console

Viewing information about nodes with application components installed and about network interfaces on nodes

Viewing the status of services supporting operation of application components

Restarting a computer that has application components installed

Using a test network packet to verify event registration

Synchronizing Server time with the time source for industrial network assets

Updating SSL connection certificates

Updating databases and application modules

Selecting an update source

Selecting the update run mode

Manually starting an update

Viewing information about update installation

Distributing access to application functions

About application user accounts

Application functions available through the web interface

Application functions available in the Console

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
- Security policies
  - Creating a new security policy
  - Saving a security policy to a folder
  - Opening a security policy from a folder
  - Applying a security policy on the Server
  - Loading a security policy from the Server to the Console
  - Viewing security policy properties
  - Changing the name of a security policy
  - About the security policy conversion tool
  - Converting and importing a security policy
- Process Control
  - Supported devices and protocols
  - Tree of devices and tags for process control
    - Devices and tags for Process Control
    - About Unknown Tag Detection
    - Enabling and disabling Unknown Tag Detection
    - Adding a process control device
    - Adding tags from the detected tag storage
    - Manually adding a tag
    - Editing the settings of a process control device or tag
    - Removing a process control device or tag
    - Searching tags
    - Importing tags and process control devices from data files
  - Selecting the monitored system commands
  - Detecting default passwords when connecting to devices
  - Process Control rules
    - About Process Control rules
    - Rules with defined conditions for tag values
    - Rules using Lua scripts
    - Creating a group in the list of Process Control rules
    - Moving an item in the list of Process Control rules
    - Renaming an item in the list of Process Control rules
    - Removing an item from the list of Process Control rules
    - Searching Process Control rules
    - Highlighting tags used in Process Control rules
- Configuring events
  - Grouping event types
  - Searching for event types
  - Creating event types
  - Changing event types
  - Configuring automatic saving of traffic during event registration
  - Deleting event types
  - About transmission of events to recipient systems
  - Adding a recipient
  - Changing the recipient settings
  - Configuring the transmission of events to recipient systems

- Removing a recipient
- Kaspersky Industrial CyberSecurity for Networks event configuration variables

Asset management

- Asset Management modes and methods
- About monitoring read/write of PLC projects
- Selecting the applied methods and changing the Asset Management mode
- Assets table
- Viewing the assets table
- Selecting assets in the assets table
- Automatically adding and updating assets
- About the asset group tree
- Creating an asset group tree
- Manually adding assets
- Merging assets
- Deleting assets
- Automatically changing the statuses of assets
- Manually changing the statuses of assets
- Viewing asset information
- Managing the arrangement of assets in the group tree
- Adding and removing labels for assets
- Editing asset information
- Adding, editing and deleting custom fields for an asset
- Viewing events associated with assets

Network Control

- Network Control learning mode
- Network Control monitoring mode
- Selecting the applied technologies and changing the Network Control mode
- Automatic generation of Network Control rules in learning mode
- Viewing the table of Network Control rules
- Selecting Network Control rules
- Manually creating Network Control rules
- Editing Network Control rule settings
- Changing the state of Network Control rules
- Deleting Network Control rules

Intrusion Detection

- Intrusion Detection rules
- Additional Intrusion Detection methods
- Enabling and disabling rule-based Intrusion Detection
- Enabling and disabling additional Intrusion Detection methods
- Viewing the table containing sets of Intrusion Detection rules
- Changing the state of sets of Intrusion Detection rules
- Loading and replacing custom sets of Intrusion Detection rules
- Removing custom sets of Intrusion Detection rules

Managing logs

- Managing the settings for storing log entries in the database
- Managing the settings for saving traffic in the database
- Enabling and disabling the user activity audit
- Changing the log level for processes

Managing technologies

Using the Kaspersky Industrial CyberSecurity for Networks API

Certificates for secure connection through the API

Creating client certificates for connection through the API

Performing common tasks

System monitoring in online mode

Information in the Assets block

Viewing detailed information about assets

Searching assets and proceeding to the Assets section

Information in the Events block

Selecting a period for displaying a histogram

Viewing detailed information about events and incidents

Searching events and incidents and proceeding to the Events section

Working with the network map

Nodes on the network map

Groups of assets on the network map

Links on the network map

Viewing details about objects

Changing the network map scale and positioning

Collapsing and expanding groups

Moving nodes and groups to other groups on the network map

Pinning and unpinning nodes and groups

Manually changing the location of nodes and groups

Automatic arrangement of nodes and groups

Filtering nodes and links by time of communication

Filtering nodes on the network map

Filtering links on the network map

Saving and loading network map display settings

Resetting the defined filter settings on the network map

Searching nodes on the network map

Viewing events associated with nodes of known assets

Viewing events associated with a link

Viewing information in the assets table for selected nodes

Viewing information in the assets table for a selected link

Monitoring events and incidents

Event severity levels

Event registration technologies

Event statuses

Table of registered events

Selecting events in the events table

Viewing events included in an incident

Filtering events

Searching events

Resetting the defined filter and search settings in the events table

Sorting events

Configuring the table of registered events

Viewing event details

Viewing information about assets associated with events

Changing the statuses of events

Setting markers

Copying events to a text editor

Exporting events to a file

Loading traffic for events

Monitoring process parameters

Viewing process parameters

Sorting tags when viewing process parameters

Application interaction with Kaspersky Security Center

Connecting to the Console from Kaspersky Security Center

Adding a license key to Kaspersky Industrial CyberSecurity for Networks from Kaspersky Security Center

Using the Kaspersky Security Center Administration Server as the source of updates

Monitoring events via Kaspersky Security Center

Types of events in Kaspersky Security Center for Kaspersky Industrial CyberSecurity for Networks events

Correspondence of Kaspersky Security Center event severity levels

Monitoring the ICS security state: Kaspersky Security Center and SCADA

Troubleshooting

An application component cannot be installed on a selected node

Application problems detected

New application message

Not enough free space on hard drive

No traffic at monitoring point

Unknown state of the application

Traffic is not being loaded for events or incidents

Preventative maintenance and adjustment operations on the ICS

Unexpected system restart

After the Kaspersky Security Center Administration Server is reinstalled, Network Agent cannot be synchronized

Unable to connect to the Server through a web browser

When connecting to the Server, the web browser displays a certificate warning

Contacting Technical Support

How to get technical support

Technical support by phone

Technical Support via Kaspersky CompanyAccount

Collecting information for Technical Support

Sources of information about the application

Appendices

Example installation of a Server and sensor

System event types in Kaspersky Industrial CyberSecurity for Networks

System event types based on Deep Packet Inspection technology

System event types based on Command Control technology

System event types based on Network Integrity Control technology

System event types based on Intrusion Detection technology

System event types based on Asset Management technology

System event types based on External technology

Files for importing custom tags and device configurations

File with descriptions of devices: devices.csv

File with descriptions of connections and protocols: connections.csv

File with descriptions of tags and variables: variables.csv

File with descriptions of enumerations: enums.csv

File with descriptions of data sets (tag sets): datasets.csv

File with descriptions of MMS protocol reports: iec61850_mms_reports.csv

File with descriptions of Sampled Values protocol messages: iec61850_sv_messages.csv

Glossary

Account role

ARP spoofing

Asset management

Command Control

Dedicated Kaspersky Industrial CyberSecurity network

Deep Packet Inspection

Device

Event

Event correlation rule

Event type

External

ICS

Incident

Industrial network

Intelligent electronic device (IED)

Intrusion Detection

Intrusion Detection rule

Kaspersky Industrial CyberSecurity for Networks Console

Kaspersky Industrial CyberSecurity for Networks Sensor

Kaspersky Industrial CyberSecurity for Networks Server

Kaspersky Industrial CyberSecurity for Networks Web Server

Link on the network map

Monitoring point

Network Control rule

Network Integrity Control

Network map

Node

Notification

PLC project

Process Control rule

Programmable Logic Controller (PLC)

SCADA

Security policy

SIEM

System command

Tag

AO Kaspersky Lab

Information about third-party code

Trademark notices

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 monitor the activity of devices in the industrial network, detect prohibited system commands transmitted or received by devices, and detect attempts to set incorrect process parameter values. The application is part of the solution known as Kaspersky Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Networks performs the following functions:

- Scans communications between industrial network devices to check their compliance with defined Network Control rules.
- Monitors industrial network devices and detects the activity of devices previously unknown to the application, as well as the activity of devices that must not be used in the industrial network or that have not shown any activity in a long time. When monitoring devices, the application can automatically refresh information about devices based on data received in network packets.
- Displays the network interactions between industrial network devices depicted as a network map. Displayed objects are visually distinguished based on various attributes (for example, objects requiring attention).
- 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.
- Analyzes industrial network traffic to see if network packets contain system commands transmitted or received by devices involved in automating an enterprise's processes (hereinafter referred to as "process control devices"). Monitors traffic to detect 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 preset network packet scan algorithms to detect signs of attacks.
- 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. Correlation rules may be updated when updates are installed.
- Saves traffic associated with registered events in the database. Traffic may be saved automatically if the saving of traffic is enabled for event types, or can be saved by requesting to load traffic.
- Can be used to work with both the GUI and API.

Distribution kit

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

- Application installation script: kics4net-deploy-<application version number>.bundle.sh
- Package for installing the Server and sensors: kics4net-<application version number>.x86_64.rpm
- Package for installing the Console: kics4net-utm-<application version number>.x86_64.rpm
- Package for installing the DBMS: kics4net-postgresql-<DBMS version number>.x86_64.rpm
- Package for installing the Intrusion Detection system: kics4net-suricata-<system version number>.x86_64.rpm
- Package for installing a web server: kics4net-webserver-<application version number>.x86_64.rpm
- Package for installing Network Agent from the Kaspersky Security Center distribution kit: klnagent64-<Network Agent version number>.x86_64.rpm
- Packages for installing the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center: kics4net-sc-plugin_<plug-in version number>_<localization code>.msi
- Package containing the set of proto files for Kaspersky Industrial CyberSecurity for Networks API: kics4net-api-<application version number>.tar.gz
- 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
- File containing information in English about third-party code (Legal Notices)

Hardware and software 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.
  - RAM: 32 GB.
  - Free space on the hard drive: 750 GB and an additional 250 GB for each monitoring point on this computer.
- Computer that will perform sensor functions:
  - CPU: Intel Core i5 / i7.
  - RAM: 4 GB, and an additional 2 GB for each monitoring point on this computer.
  - Free space on the hard drive: 50 GB and 250 GB for each monitoring point on this computer.

When using sensors, the bandwidth of the dedicated Kaspersky Industrial CyberSecurity network between the Server and sensors must be at least twice the bandwidth of the industrial network.

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

- CentOS 7.6.1810 operating system.

  > When installing the operating system, we recommend that you allocate the entire hard drive (minus the space required for the boot and swap partitions) to the system (root) partition.

- The same version of operating system must be installed on all computers where application components are installed.
- To install application components, the following software must be installed in the CentOS 7.6.1810 operating system:
  - The KDE desktop environment version included in the CentOS 7.6.1810 operating system.
  - Python 2.7.
  - Chrony time synchronization package version 3.1 or later.
- On the computer that will perform Server functions, the mail server (Mail Transfer Agent) must be correctly configured to send emails to the notification recipients configured in the Console.

> 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.

To install the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center, the Windows® update KB2999226 must be installed on the computer hosting the Kaspersky Security Center Administration Server. Installation of this update is required if the problems fixed by this update are relevant for the installed version of the operating system and configuration of the installed software on the computer hosting the Administration Server (please refer to the description of the specific update).

To connect to the web server, you can use the following web browsers:

- Google Chrome™ version 78 or later.
- Mozilla™ Firefox™ version 70 or later.
- Microsoft® Edge version 44 or later.

Kaspersky Industrial CyberSecurity for Networks is compatible with the following versions of applications that are part of the Kaspersky Industrial CyberSecurity solution:

- Kaspersky Security Center 10 with Service Pack 3 or Kaspersky Security Center 11.
- Kaspersky Industrial CyberSecurity for Nodes version 2.5 or 2.6.

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 assets and track changes to asset information based on data received in network packets. To automatically receive information about assets, the application analyzes industrial network traffic according to the rules for identifying information about devices and the protocols of communication between devices. 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. Asset Management can be configured when working with the assets table. Some configuration capabilities are also available when working with the network map.

- Network Control. This functionality lets you monitor interactions between assets of the industrial network. Detected interactions are checked to see if they match defined Network Control rules. When the application detects an interaction that is described in an active Network Control 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 assets. 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. Intrusion Detection rules and embedded network packet scan algorithms are used to detect such activity. When the conditions defined in an active Intrusion Detection rule are detected in traffic, the application registers a rule-triggering event. Using the embedded network packet scan algorithms, the application detects signs of falsified addresses in ARP packets and various anomalies in the TCP and IP protocols.

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 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 monitoring the system in online mode, you can view information about assets requiring attention, and information about events and incidents with the most recent time of last occurrence.

- Display data on the network map. This functionality lets you visually display detected interactions between assets of the industrial network. When viewing the network map, you can quickly identify problematic objects or objects with other attributes and view information about these objects. To conveniently present information, you can automatically or manually arrange assets on the network map.

- Display information about events and incidents. This functionality lets you load registered events and incidents from the Server database. 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 information for monitoring process parameters. This functionality lets you view the values of process parameters detected in traffic at the current time. Information about settings is presented in the form of a table whose values are automatically updated.

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 monitoring points. This functionality lets you add monitoring points to the application to receive traffic from the industrial network. You can also use this functionality to temporarily pause and resume monitoring of industrial network segments by disabling and enabling the corresponding monitoring points (for example, while conducting preventative maintenance and adjustment operations for the ICS).

- Manage technologies. This functionality lets you enable and disable the use of technologies and methods for industrial network traffic analysis, and change the operating mode of technologies and methods. You can enable, disable, and change the operating mode of technologies and methods independently of each other.

- 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. When configuring event types, you can also add event types for event registration using methods of the Kaspersky Industrial CyberSecurity for Networks API.

- 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 log levels for process logs.

- 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 methods provided by the Kaspersky Industrial CyberSecurity for Networks API, you can obtain data on events and tags, send events to Kaspersky Industrial CyberSecurity for Networks API, 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.

It is also recommended to restrict access to hardware on which the application is running.

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

- Restrict access to computers on which the Kaspersky Industrial CyberSecurity for Networks Server and sensors are installed, and restrict access to the network equipment of the dedicated network.
- Grant access to personnel authorized to install and configure the Server's and sensors' equipment and software, and to users of the application.
- Use hardware or a security service to control physical access to the equipment running the application.
- Restrict access to network equipment used for receiving data from the industrial network and for the interaction of application components.
- Use an alarm system to monitor access to restricted rooms.
- Install video surveillance in 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 intranet:

- Protect traffic within the 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.
- Terminate the Server connection session before the user closes the web browser or Application Console.

  To force termination of a connection session in the web browser, you need to use the **Log out** option in the user menu. To force termination of a connection session in the Application Console, you need to close the Console window.

What's new

Kaspersky Industrial CyberSecurity for Networks 2.9 has the following new capabilities and refinements:

- Asset group tree – you can now manage the tree of asset groups. You can put known assets into groups to organize these assets according to their purpose, location, or any other attribute.
- Labels for assets – you can now add or remove labels for known assets. Labels can contain any user-defined text descriptions of assets.
- Manage monitoring points – you can now add or remove monitoring points on nodes of the Server and sensors without having to reinstall application components. To pause or resume traffic processing, you can simply disable or enable monitoring points (the functionality for pausing and resuming the Server or sensors has been discontinued).
- Identification of protocols based on the contents of network packets – for Network Control and event registration, the application can now identify individual application-layer protocols based on the data comprising the payload of network packets.
- Unknown Tag Detection – the application can now detect and save information about tags that are not included in the security policy but are associated with process control devices.
- Expanded functionality for saving traffic for events – you can now enable saving of traffic for incidents (the traffic for all events within incidents will also be saved) and obtain traffic from temporary dump files if the traffic is not found in the database (by requesting to load traffic).
- Collapse the menu on the web interface page – you can now collapse and expand the menu in the left part of the page of the application web interface. Use the buttons to collapse or expand the menu.
- Select all items in tables – you now have the capability to quickly select all items that satisfy the current filter and search settings in the assets table, Network Control rules table, and events table. You can select all items by using the key combination CTRL+A or by using the check box in the header of the left-most column of the table.
- Display the number of unprocessed events – an information panel has been added to the **Events** section to display information about the number of events that have the *New* or *In progress* status.
- Search nodes on the network map.
- Save and load network map views (display settings).
- Use Kaspersky Security Center to download updates – you can now select the Kaspersky Security Center Administration Server as the source of updates for application modules and databases.
- Add a license key from Kaspersky Security Center – you can now add a license key to Kaspersky Industrial CyberSecurity for Networks using the functionality provided by Kaspersky Security Center for automatic distribution of license keys.
- Expanded functionality of the application programming interface (API) – you can now receive asset information from the assets table.
- Information about working with the application is provided in Online Help format – information about installing, configuring, and using Kaspersky Industrial CyberSecurity for Networks (including about using the Kaspersky Industrial CyberSecurity for Networks API) is published on the Kaspersky Online Help page. Online Help provides convenient tools for searching, viewing, and printing information, and for receiving electronic documents in PDF format.

- Extended support for application layer protocols: there are now additional capabilities for analyzing traffic of supported application layer protocols and new supported protocols have been added.

- Extended hardware support: new supported devices have been added.

Application architecture

Kaspersky Industrial CyberSecurity for Networks includes the following components:

- The *Server* is the main component that receives and processes industrial network traffic information, saves it and provides data (for example, events and asset information). The application may have only one Server.
- The *Web Server* provides the interface for connecting to the Server through a web browser (web interface). Application users can use the web interface to view data provided by the Server and manage operation of the application. The web server is installed on the computer that acts as the Server. Certificates are used for a secure connection with the Web Server.
- The *Console* provides the graphical interface for connecting to the Server. Application users can use the Console to configure the functionality that cannot be configured through the web interface. The Console is installed on the computer that acts as the Server.
- A *sensor* receives a copy of industrial network traffic, processes the obtained data and relays it to the Server. Sensors are installed on separate computers (not on a computer that performs Server functions). The application can have up to 32 sensors.

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

- Receives traffic information from Kaspersky Industrial CyberSecurity for Networks sensors and/or independently receives a copy of industrial network traffic.
- Registers events and saves them in the database.
- Monitors application performance.
- Monitors the activities of application users.
- Processes incoming requests from the Web Server and the Console, and provides the requested data.
- Transmits events to Kaspersky Security Center and recipient systems (for example, to a SIEM system).

The Web Server interacting with the Server provides the following capabilities to an application user:

- View information about assets, events, and process parameters in online mode.
- View and process registered events.
- View and modify information about controlled assets.
- View information about interactions between assets.
- Configure application functions.
- View information about application operation.
- View user activity audit entries.

The Console provides the following capabilities to an application user:

- Configure Process Control rules.

- Create a list of registered event types.
- Configure transmission of events to recipient systems.
- Configure Intrusion Detection rules.
- Configure updates of application modules and databases.

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

- Processes incoming industrial network traffic.
  - Extracts information about device communications and process parameters from industrial network traffic.
  - Identifies signs of attacks in industrial network traffic.
- Registers events based on the results of industrial network traffic processing.
- Relays events, information about traffic, and information about process parameters to the Kaspersky Industrial CyberSecurity for Networks Server.

Sensors and/or the Server receive a copy of industrial network traffic from *monitoring points*. 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 32 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).

Application users can connect to the Server through the web interface or the Console on a computer that performs Server functions, or connect remotely. However, only a remote desktop system can be used to work remotely with the Console.

It is recommended to use a *dedicated* Kaspersky Industrial CyberSecurity network for the connections between nodes that have installed components of Kaspersky Industrial CyberSecurity for Networks and other components of Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity for 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 through the web interface.
- Computer hosting Kaspersky Industrial CyberSecurity for Nodes.
- Computer hosting Kaspersky Security Center.

- Network switch.

Installing and removing the application

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

Common deployment scenarios

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

- Installation of only a Server without sensors
- Installation of a Server with sensors

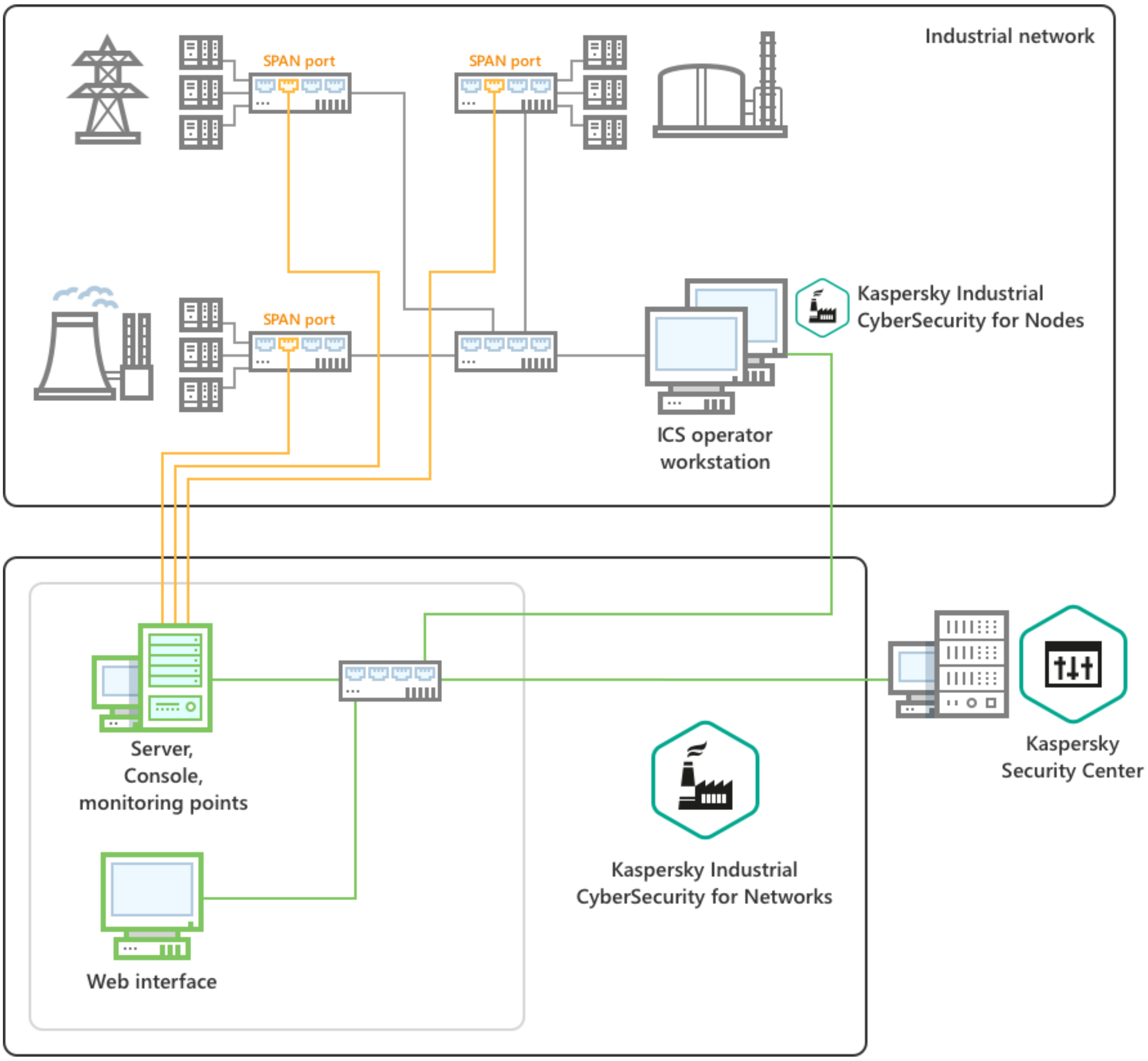
The Kaspersky Industrial CyberSecurity for Networks Server is installed together with the Console. Installation of the Server is accompanied by installation of a Web Server that facilitates connection to the Server through the web interface.

> 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 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 section.

Installing a Server without sensors

When installing a Server without sensors, all industrial network traffic must be received by the computer that performs Server functions. You can apply this installation method if the computer has a sufficient number of network interfaces that will receive traffic from all segments of the industrial network. After the application is installed, you need to add monitoring points to these network interfaces. Monitoring points are added when connected to the Server through the web interface. You can use no more than 4 monitoring points on the Server.

The example in the figure below shows deployment of the 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 in 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.


Industrial network
SPAN port
SPAN port
SPAN port
Kaspersky Industrial CyberSecurity for Nodes
ICS operator workstation
Server, Console, monitoring points
Kaspersky Security Center
Kaspersky Industrial CyberSecurity for Networks
Web interface

Example deployment of a Server without sensors

Installing the Server and sensors

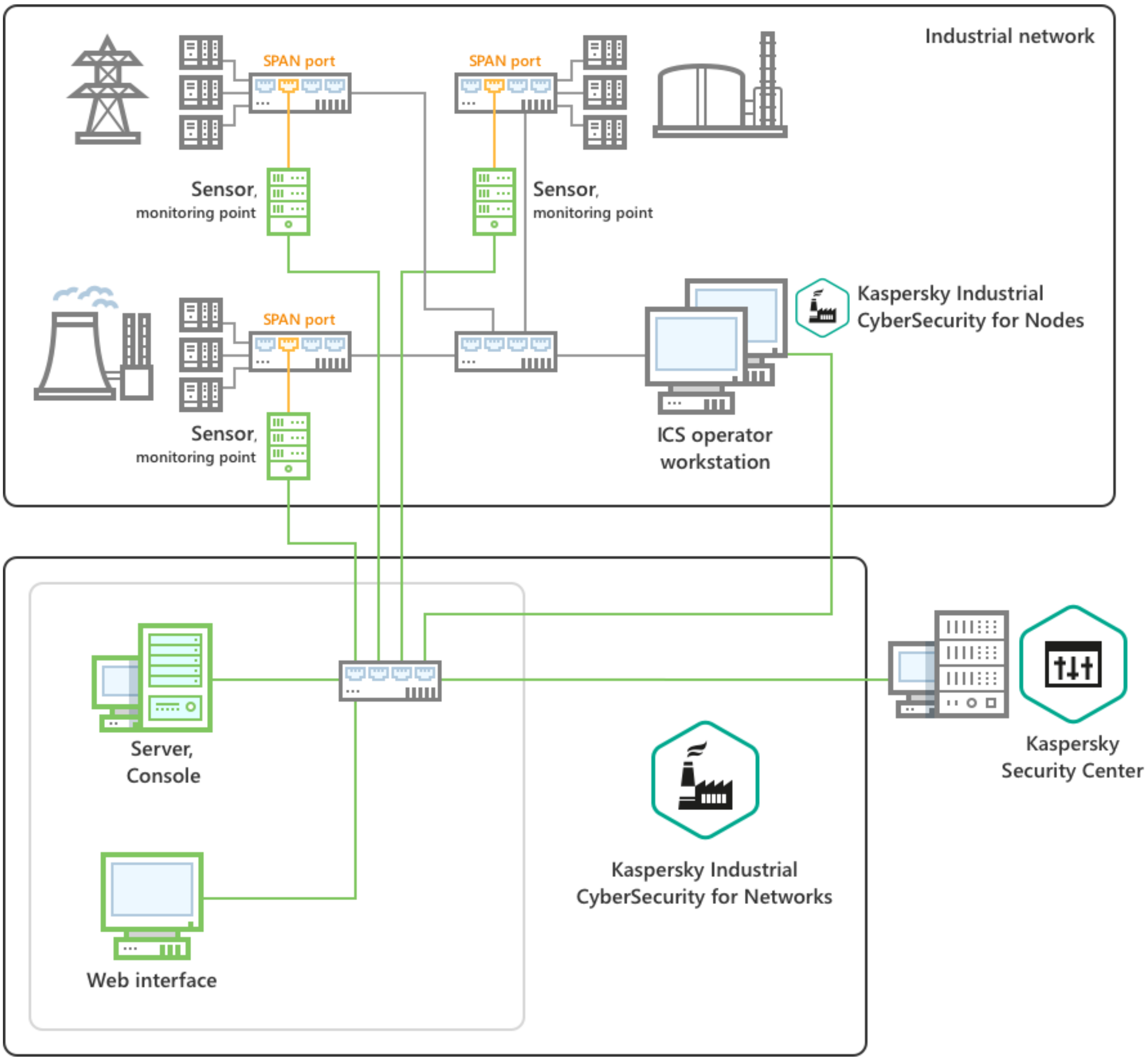
You can use from 2 to 33 computers for installing the Server and sensors. The Server is installed on one of the computers. The sensors are installed on the other computers. These sensors will receive traffic from their respective segments of the industrial network.

After the application is installed, you must add monitoring points on all computers that have sensors installed. If the computer hosting the Server has a network interface connected to the industrial network, you can also add a monitoring point to this network interface. Monitoring points are added when connected to the Server through the web interface.

If the computer has multiple network interfaces that receive traffic from different segments of the industrial network, you will have to add a monitoring point to each of these interfaces. However, you need to adhere to the limits on the maximum number of monitoring points:

- No more than 8 monitoring points on a sensor
- No more than 4 monitoring points on the Server
- No more than 32 monitoring points in the application

The example in the figure below shows deployment of the 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 in 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

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. Then make sure that the following conditions have been fulfilled:

- The computers have network access, and access over SSH is configured and open.
- You can use the system on the computer from which installation is performed as a user without root permissions.

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.

To prepare computers for installation of the application:

1. Prepare the user accounts:

   - 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. This information will be needed when installing the application.

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

   - On the computer that will perform Server functions, create local user accounts (or select existing user accounts) that will be allowed to start the Application Console. These user accounts will not require root privileges to execute commands. Local user accounts will be used to sign in to the system and to subsequently start the Application Console (however, after starting the Console, you will also need to provide the application user credentials, which might not match the credentials of the local user account). Remember the names of the created or selected local user accounts. This information will be needed when installing the application.

     > The local user accounts that need to be allowed to start the Application Console are indicated when configuring the application installation settings. These user accounts are automatically included into the special group named kics4net, which is created in the operating system during installation of the application. After the application is installed, you can use the standard tools of the operating system to manually add the necessary user accounts to the kics4net group.

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 installation will be performed, use the SSH protocol to connect to each computer to which 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. On the computer from which the installation will be performed, create a folder for storing the installation files.

5. Copy the following files from the Kaspersky Industrial CyberSecurity for Networks distribution kit to the folder you created:

   - Application installation script kics4net-deploy-<application version number>.bundle.sh
   - Package for installing the Server and sensors: kics4net-<application version number>.x86_64.rpm
   - Package for installing the Console: kics4net-utm-<application version number>.x86_64.rpm
   - Package for installing the DBMS: kics4net-postgresql-<DBMS version number>.x86_64.rpm
   - Package for installing the Intrusion Detection system: kics4net-suricata-<system version number>.x86_64.rpm
   - Package for installing a web server: kics4net-webserver-<application version number>.x86_64.rpm
   - Package for installing Network Agent from the Kaspersky Security Center distribution kit: klnagent64-<Network Agent version number>.x86_64.rpm

     > The package for installing Network Agent is required if you want to monitor the state of the application, receive a license key, and download application updates via Kaspersky Security Center. Network Agent is a Kaspersky Security Center component that enables interaction between the Kaspersky Security Center Administration Server and Kaspersky applications that are installed on a specific node (workstation or server). For detailed information on Network Agent, please refer to the Kaspersky Security Center Help system.

   The folder with the listed files will be required during installation, modification of installation settings, and uninstallation of the application.

Installation menu commands

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

You can use the installation menu to create or modify the application installation configuration and run the installation procedure in the defined configuration.

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 management commands
- Sensor management commands
- General installation commands

- Installation menu exit commands

Installation menu commands for Server management

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.
  - Enter the IP address for connections to the Server – defines the IP address that will be used by other components (for example, sensors) to connect to the Server. By default, this is the IP address of the node used for installing the Server.
  - Enter Server name – defines the name of the Server within 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 Latin 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.
  - 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. When adding the capability for application interaction with Kaspersky Security Center, you must specify the IP address / name of the computer with Kaspersky Security Center and the SSL port for the connection.

    > 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.
  - Enter the IP address or name of the computer with the web server – defines the IP address or computer name of the Server for connecting through the web interface.
  - Enter the web server port number – defines the port number for connecting through the web interface. If the default port number (443) is specified, the user only needs to enter the IP address or computer name when connecting through a web browser. In this case, the HTTPS protocol and the port number are automatically determined.
  - Enter an application user name – defines the user name for connecting to the Server and working with the application. You can enter any unique name using uppercase and lowercase letters of the Latin 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 specified user name will be used only when connecting to the Server through the web interface or in the Application Console. This user does not have to be registered as an operating system account on the Server computer or other computer. You are prompted to enter a new password for the user when installing the Server (unless another application user account with the same name is found).

  - **Use self-signed certificates to connect to web server** – lets you select the option to use certificates for protecting the connection through the web interface. You can use a self-signed certificate of the Web Server or a certificate that was published by a trusted certificate authority (hereinafter referred to as a "trusted certificate"). If you want to select the option to use a self-signed certificate, you must enter `y` at this prompt. A self-signed certificate will be created during installation of the Server. If you want to select the option to use a trusted certificate, you must enter `n` at this prompt and then `y` at the prompt to **Use trusted certificates to connect to web server**. To load a trusted certificate, you must specify the path to the trusted certificate file. This file will be copied to the folder containing web server certificates during installation of the Server. If neither option was selected (`n` has been entered at both prompts), during installation of the Server either a self-signed certificate will be created or the existing certificate in the folder containing web server certificates will be used (if a certificate remained from a previously installed Server).

    > If you want to use a trusted certificate in the application, it must be issued for the same IP address or computer name that will be indicated by application users when connected through the web interface. To load a trusted certificate, you can use a PFX file containing the saved trusted certificate and private key. The file must be created without a defined password for accessing the contents.

  - **Enter the operating system user name for starting the Console** – defines the operating system user name that will be allowed to start the Kaspersky Industrial CyberSecurity for Networks Console. After entering a user name, the **Specify the name of one more user** prompt appears. If you need to allow another user to start the Console, you need to type `y` at this prompt and then specify the name of the other user (this way you can specify multiple users consecutively). After you have specified the names of all relevant users, you need to type `n` at the **Specify the name of one more user** prompt. Permission to start the Console is provided by adding a user to the kics4net group during installation of the Server.

    > The specified user is provided the permission to only start the Console. To work with the Console, the application user credentials must be entered into the prompt that is displayed immediately after the Console is started.

- **Change Server settings** – modifies the settings of the added Server. You can use this menu item to change the main Server settings that can be edited (for example, Web Server settings) and configure advanced settings. After selecting this item, you will see a submenu in which you can change the following settings:

  - **Change Server name** – changes the name of the Server within Kaspersky Industrial CyberSecurity. This menu item is analogous to the **Enter Server name** item in the **Add Server** menu.

  - **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 autostart of kics4net** – disables autostart of the kics4net service when the operating system starts.

- **Set occupied space limit in gigabytes** – sets a 500 GB limit on the maximum space that can be occupied by application files on the hard drive of the node. This menu item is available if the current limit is defined as a percentage. When you select this item, you can change the default value within the range of 12–100000 GB. However, if the free space on the node during installation of application components is less than the defined limit (including the space occupied by existing application files remaining from the previous installation of application components), the installation ends with an error.

- **Set occupied space limit as a percentage of free disk space** – enables a limit equal to 90% of free disk space as the maximum space that can be occupied by application files on the hard drive of the node. This menu item is available if the current limit is set in gigabytes. When you select this item, you can change the default value within the range of 1–100%. During installation of application components, the application will determine the free disk space on the hard drive of this node. The application will then convert the defined value into gigabytes and save the obtained result as the active limit. However, if the free space on this node during installation of application components is less than 12 GB (including the space occupied by existing application files remaining from the previous installation of application components), the installation ends with an error.

- **Change the set occupied space limit** – changes the current maximum space that can be occupied by application files on the hard drive of the node. The range of possible values depends on the measurement units of the currently defined limit (as a percentage or in gigabytes). For details about determining the free disk space on a hard drive depending on the measurement units, please refer to the sections titled **Set occupied space limit in gigabytes** and **Set occupied space limit as a percentage of free disk space**.

- **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.

- **Change the IP address or name of the computer with Kaspersky Security Center** – modifies the IP address / name of the computer with Kaspersky Security Center (if the capability for application interaction with Kaspersky Security Center has been added).

- **Change SSL port number of computer with Kaspersky Security Center** – modifies the SSL port used for connecting to the computer with Kaspersky Security Center (if the capability for application interaction with Kaspersky Security Center has been added).

- **Disable the capability for application interaction with Kaspersky Security Center** – removes the capability for application interaction with Kaspersky Security Center.

- **Change the settings for connecting to the Server via API** – changes the settings for inbound and outbound connections using the Kaspersky Industrial CyberSecurity for Networks API. When modifying settings, you can specify another computer name on which the gRPC server is running. This name must match the name of the computer that performs Server functions. You can also generate new certificates for connecting to Kaspersky Industrial CyberSecurity for Networks through the API (if the computer name was changed or if you need to update the current certificates for other reasons).

- **Change the IP address or name of the computer with the web server** – modifies the IP address or computer name of the Server for connecting through the web interface.

- **Change the web server port number** – modifies the port number for connecting through the web interface. If the default port number (443) is specified, the user only needs to enter the IP address or computer name when connecting through a web browser. In this case, the HTTPS protocol and the port number are automatically determined.

- **Change the application user name** – changes the previously defined user name for connecting to the Server and working with the application. You can enter any unique name using uppercase and lowercase letters of the Latin 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 specified user name will be used only when connecting to the Server through the web interface or in the Application Console. This user does not have to be registered as an operating system account on the Server computer or other computer. When changing the name of an existing application user, the old user account is not deleted, and a new user account is created. You are prompted to enter a new password for the user when reinstalling the application (unless another application user account with the same name is found).

- **Change web server certificate settings** – modifies the settings for using certificates to protect the connection through the web interface. Certificate usage settings are changed similarly to the **Use self-signed certificates to connect to web server** option in the **Add Server** menu.

- **Add an operating system user for starting the Console** – adds an operating system user that will be allowed to start the Kaspersky Industrial CyberSecurity for Networks Console. This menu item is analogous to the **Enter the operating system user name for starting the Console** item in the **Add Server** menu.

- **Change the operating system user name for starting the Console** – changes the added operating system user name that is allowed to start the Kaspersky Industrial CyberSecurity for Networks Console (for example, if the name of the operating system user account changed).

- **Remove the operating system user for starting the Console** – revokes the operating system user's permission to start the Console. Permission is revoked by removing the user from the kics4net group during reinstallation of the application.

- **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.

Installation menu commands for sensor management

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 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 sensor.

  - **Enter sensor name** – defines the name of the sensor within Kaspersky Industrial CyberSecurity. 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 Latin 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.

- **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 (for example, its name) and 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:

  - **Change sensor name** – changes the name of the sensor within Kaspersky Industrial CyberSecurity. This menu item is analogous to the **Enter sensor name** item in the **Add sensor** menu.

  - **Specify an additional user to run the installation** – defines an additional user account that will be used to run the installation on the sensor node. This menu item is analogous to the **Specify an additional user to run the installation** item in the **Change Server settings** menu.

  - **Enable hardware Watchdog** – enables use of the hardware Watchdog. This menu item is analogous to the **Enable Hardware Watchdog** item in the **Change Server settings** menu.

  - **Disable autostart of kics4net** – disables autostart of the kics4net service when the operating system starts.

  - **Set occupied space limit in gigabytes** – sets a 500 GB limit on the maximum space that can be occupied by application files on the hard drive of the node. This menu item is available if the current limit is defined as a percentage. When you select this item, you can change the default value within the range of 8–100000 GB. However, if the free space on the node during installation of application components is less than the defined limit (including the space occupied by existing application files remaining from the previous installation of application components), the installation ends with an error.

  - **Set occupied space limit as a percentage of free disk space** – enables a limit equal to 90% of free disk space as the maximum space that can be occupied by application files on the hard drive of the node. This menu item is available if the current limit is set in gigabytes. When you select this item, you can change the default value within the range of 1–100%. During installation of application components, the application will determine the free disk space on the hard drive of this node. The application will then convert the defined value into gigabytes and save the obtained result as the active limit. However, if the free space on this node during installation of application components is less than 8 GB (including the space occupied by existing application files remaining from the previous installation of application components), the installation ends with an error.

  - **Change the set occupied space limit** – changes the current maximum space that can be occupied by application files on the hard drive of the node. The range of possible values depends on the measurement units of the currently defined limit (as a percentage or in gigabytes). For details about determining the free disk space on a hard drive depending on the measurement units, please refer to the sections titled **Set occupied space limit in gigabytes** and **Set occupied space limit as a percentage of free disk space**.

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

General installation menu 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 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.

- **Change interface language** – defines the localization language for components of Kaspersky Industrial CyberSecurity for Networks (Console, sensors, and Server) and the data that comes from them.

- **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 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 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 installation script, and exit without installing components.

- **Exit without saving settings** – terminate the application installation script without saving changes to the installation settings file.

Application installation procedure

Application components are installed using files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks. Prior to installing components, you must perform the necessary actions to prepare for application installation.

Installation of components is started by the application installation script kics4net-deploy-<application version number>.bundle.sh. The script uses data that was saved in the installation settings file.

During installation of the application, by default the script verifies the checksums of packages in the folder containing the saved files from the distribution kit. This lets you verify the integrity of files from the application installation packages by comparing the calculated checksums of packages with their reference values. If a calculated checksum for even one package does not match the reference value, the installation script stops.

> It is recommended to install the application with validation of the package checksums enabled. If necessary, you can disable validation of package checksums. However, correct installation of application components cannot be guaranteed if you do so.

To install Kaspersky Industrial CyberSecurity for Networks on computers:

1. On the computer from which the installation will be performed, go to the folder containing the saved files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks.

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

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

> If for some reason you need to enable validation of the checksums of packages used for application installation, you can enter the script startup command with the `--skip-checksum-validation` switch. This switch is intended only for testing and must not be used during normal installation of the application.

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. To change the localization language of components, use the **Change interface language** menu item.

4. If the application installation script was run without the `--skip-checksum-validation` switch, after selecting the language for the installation menu, the script runs a verification of the checksums of packages in the folder containing the saved files from the distribution kit. Wait for validation of the package checksums to complete.

   If a calculated checksum for even one package does not match the reference value, the installation script stops. In this case, replace the corrupted files with the original files from the distribution kit and run the application installation script again.

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

   The main installation menu appears on the screen.

6. Perform the following actions:

   a. Click the **Add Server** menu item to add the Kaspersky Industrial CyberSecurity for Networks Server. Specify the IP addresses, name, and other main settings for the Server in the prompts that appear.

      You can configure advanced settings for the Server (for example, change the default limit on occupied disk space). Use the **Change Server settings** menu item to configure advanced settings.

   b. If the Server is installed with sensors, use the **Add sensor** menu item to add nodes of sensors. For the sensors, specify the IP addresses and names in the prompts that appear.

      You can configure advanced settings for sensors (for example, change the default limit on occupied disk space). Use the **Change sensor settings** menu item to configure advanced settings.

   c. Use the **Change the user running the installation** menu item to specify the user account with root privileges that will be used to install the application 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.

   d. Using the **Change interface language** menu item, select the localization language for components of Kaspersky Industrial CyberSecurity for Networks.

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

8. When the screen displays a message prompting you to read the terms of the End User License Agreement and Privacy Policy, press **ENTER**.

   The text of the End User License Agreement will appear on the screen.

9. Please carefully read the End User License Agreement.

The text of the End User License Agreement is displayed in the text terminal program known as less. After you are finished viewing the End User License Agreement, the screen will display a menu in which you can select your next actions.

10. If you fully agree to the terms of the End User License Agreement, select **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.

> If you do not accept the terms of the End User License Agreement, cancel application installation by selecting **I decline the terms of the End User License Agreement**.

11. When you see a message about viewing the Privacy Policy, press `ENTER`.

    The text of the Privacy Policy will appear on the screen.

12. Please carefully read the Privacy Policy.

    The text of the Privacy Policy is displayed in the text terminal program known as less. After you are finished viewing the Privacy Policy, the screen will display a menu in which you can select your next actions.

13. If you fully accept the terms of the Privacy Policy, select **I understand and agree that my data will be processed and transmitted (including to third-party countries) in accordance with the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.

> If you do not agree to the terms of the Privacy Policy, cancel application installation by selecting **I decline the terms of the Privacy Policy**.

After you accept the terms of the Privacy Policy, the screen will prompt you to enter the password of the user running the installation.

14. 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 `SUDO password` prompt.

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

15. When the prompt appears for entering the password of the application user (the user name that was specified during configuration of the Server), enter the new user password.

    You can use uppercase and lowercase letters of the Latin alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

    The password must meet the following requirements:

    - Must contain from 8 to 20 characters.
    - Must contain one or more uppercase letters.
    - Must contain one or more lowercase letters.
    - Must contain one or more numerals.

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

After installation is complete, Kaspersky Industrial CyberSecurity for Networks does not monitor the industrial network (monitoring points have not been added to network interfaces of nodes that have application components installed). To use the application, you need to perform the necessary actions to prepare the application for operation.

Viewing the End User License Agreement and Privacy Policy

You can view the terms of the End User License Agreement and Privacy Policy as follows:

- During the installation of Kaspersky Industrial CyberSecurity for Networks.
- By reading the files named license_en.txt and privacy_policy_en.txt. These files are included in the application distribution kit, and are saved in the application installation folder.

During the installation of Kaspersky Industrial CyberSecurity for Networks, the texts of the End User License Agreement and Privacy Policy are displayed using the text terminal program known as "less". This program provides the capability to scroll through text, perform a search, copy, and perform other actions on text, except for editing.

When viewing the End User License Agreement or Privacy Policy, the lower part of the screen displays an information bar containing the following data:

- Document name.
- Sequence number of the top line displayed.
- Main keyboard shortcuts for navigating through the text (cursor control keys).
- Key for Help on application commands (**H**).
- Key for quitting the program (**Q**).

After the End User License Agreement or Privacy Policy is loaded, the installer waits for the end of text viewing in the "less" program. Text viewing in the "less" program ends in the following cases:

- An attempt is made to scroll the text further down than its last line.
- The **Q** key is pressed to quit the program.

After the text of the End User License Agreement or Privacy Policy has been viewed, the installer displays a menu in which you can select your next actions. When necessary, you can display the text again by selecting the **Read the terms of the End User License Agreement again** or **Read the terms of the Privacy Policy again** menu item.

Reconfiguring and reinstalling the application

Reinstallation of components of Kaspersky Industrial CyberSecurity for Networks may be required for the following purposes:

- To add a new sensor.

- To change the settings of the Server or sensors.
- To change the application localization language.

Like the installation procedure, reinstallation of components of Kaspersky Industrial CyberSecurity for Networks is performed using the application installation script named kics4net-deploy-<application version number>.bundle.sh.

> To reinstall application components, the script 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 installation script searches for a copy of the file on the computer and on other computers that have application components installed.

To reinstall components of Kaspersky Industrial CyberSecurity for Networks:

1. Run the application installation script by completing steps 1–4 of the installation procedure.
2. In the menu for selecting the installation option, select **Edit settings of current installation**.

   The main 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 install the application 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.
   - Using the **Change interface language** menu item, select the localization language for components of Kaspersky Industrial CyberSecurity for Networks.
4. When finished configuring the settings, select **Save settings and start installation**.
5. If the previous installation of Kaspersky Industrial CyberSecurity for Networks was performed by a different user:

   a. When the screen displays a message prompting you to read the terms of the End User License Agreement and Privacy Policy, press **ENTER**.

      The text of the End User License Agreement will appear on the screen.

   b. Please carefully read the End User License Agreement.

      The text of the End User License Agreement is displayed in the text terminal program known as less. After you are finished viewing the End User License Agreement, the screen will display a menu in which you can select your next actions.

c. If you fully agree to the terms of the End User License Agreement, select **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.

> If you do not accept the terms of the End User License Agreement, cancel application installation by selecting **I decline the terms of the End User License Agreement**.

d. When you see a message about viewing the Privacy Policy, press **`ENTER`**.

The text of the Privacy Policy will appear on the screen.

e. Please carefully read the Privacy Policy.

The text of the Privacy Policy is displayed in the text terminal program known as less. After you are finished viewing the Privacy Policy, the screen will display a menu in which you can select your next actions.

f. If you fully accept the terms of the Privacy Policy, select **I understand and agree that my data will be processed and transmitted (including to third-party countries) in accordance with the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.

> If you do not agree to the terms of the Privacy Policy, cancel application installation by selecting **I decline the terms of the Privacy Policy**.

After you accept the terms of the Privacy Policy, the screen will prompt you to enter the password of the user running the installation.

6. 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 `SUDO password` prompt.

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

7. When the prompt appears for entering the password of the application user (the user name that was specified during configuration of the Server), enter the new user password. The password prompt is displayed if the specified user name does not match the user name of any other application user.

   You can use uppercase and lowercase letters of the Latin alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

   The password must meet the following requirements:

   - Must contain from 8 to 20 characters.
   - Must contain one or more uppercase letters.
   - Must contain one or more lowercase letters.
   - Must contain one or more numerals.

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

Installing the application in non-interactive mode

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

> Installation of Kaspersky Industrial CyberSecurity for Networks in non-interactive mode implies that you accept the terms of the End User License Agreement and Privacy Policy. During a non-interactive installation, the texts of the End User License Agreement and Privacy Policy are not displayed. You must become familiar with the terms of the End User License Agreement and Privacy Policy by reading the license_en.txt and privacy_policy_en.txt files that are included in the application distribution kit.

> If you accept the terms of the End User License Agreement and understand and agree that your data will be processed and transmitted (including to third-party countries) in accordance with the Privacy Policy, and if you confirm that you have fully read and understand the terms of the Privacy Policy, you can install the application in silent mode (non-interactive mode) in accordance with the parameters described below.

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

To prepare an installation settings file using the application installation script:

1. Configure the installation settings by completing steps 1-6 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 installation settings file into a different folder.

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

> During installation of application components in non-interactive mode, there is no validation of the checksums of packages in the folder containing the saved files from the distribution kit. You can verify the checksums of packages by completing steps 1–4 of the installation procedure prior to starting installation of components in non-interactive mode.

To install application components in non-interactive mode:

1. On the computer from which the installation will be performed, go to the folder containing the saved files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks.
2. Enter the following command:

   ```
   bash kics4net-deploy-<application version number>.bundle.sh \
   --silent-mode --accept-eula --accept-privacy-policy
   ```

   where:

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

- `--accept-eula` – accepts the terms of the End User License Agreement (mandatory parameter).
- `--accept-privacy-policy` – accepts the terms of the Privacy Policy (mandatory parameter).

In addition to the mandatory settings listed above, you may also specify the following settings for running the installation script:

- `-i <path to the installation settings file>` – indicates the full path and name of the 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.

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

3. 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 `SUDO password` prompt.

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

4. When the prompt appears for entering the password of the application user (the user name that was specified during configuration of the Server), enter the new user password. The password prompt is displayed if the specified user name does not match the user name of any other application user.

   You can use uppercase and lowercase letters of the Latin alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

   The password must meet the following requirements:

   - Must contain from 8 to 20 characters.
   - Must contain one or more uppercase letters.
   - Must contain one or more lowercase letters.
   - Must contain one or more numerals.

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 installation script kics4net-deploy-<application version number>.bundle.sh.

You can use the application installation 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 application installation script performs actions that harden the security on all computers on which application components are installed.

> To reinforce security, the script 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 installation script searches for a copy of the file on the computer and on other computers that have application components installed.

To reinforce the security of computers that have application components installed:

1. On the computer from which the installation was performed, go to the folder containing the saved files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks.
2. Enter the following command:

   ```
   bash kics4net-deploy-<application version number>.bundle.sh \
   --harden <parameter>
   ```

   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 `SUDO password` invitations, enter the password for the user account that is used to run the installation.

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

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

The Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center (hereinafter also referred to as the "administration plug-in") must be installed on the computer on which the Kaspersky Security Center Administration Server is installed. The administration plug-in needs to be installed using an account that belongs to the group of local administrators.

You can install the administration plug-in in one of the following ways:

- Using the Setup Wizard.
- From the command line.

After installation, the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center appears in the list of installed administration plug-ins in the properties of the Kaspersky Security Center Administration Server. For detailed information on working with the Kaspersky Security Center Administration Server, please refer to the Kaspersky Security Center Help system.

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 from the Kaspersky Industrial CyberSecurity for Networks distribution kit.

   Run the file with the localization code that matches the localization language of Kaspersky Security Center.

2. Follow the instructions of the Setup Wizard.

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 from the Kaspersky Industrial CyberSecurity for Networks distribution kit.

3. Enter the following command in the command line:

   ```
   kics4net-sc-plugin_<plug-in version number>_<localization code>.msi <settings for
   starting MSI files>
   ```

   where:

   - `<localization code>` – localization code of the administration plug-in. Run the file with the localization code that matches the localization language of Kaspersky Security Center.

   - `<settings for starting MSI files>` refers to one or several standard startup settings provided for Windows Installer. You can receive information about available settings by running a file with the `/help` setting.

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 stages:

1. Adding monitoring points

2. Adding application users

3. Adding an update license key

4. Configuring updates of application modules and databases

5. Creating a security policy

6. Configuring Process Control

7. Configuring the list of event types

8. Applying a security policy

9. Configuring Intrusion Detection

10. Configuring Asset Management

11. Configuring Network Control

Upgrading from a previous version of the application

To upgrade from a previous version of Kaspersky Industrial CyberSecurity for Networks, you must first fully remove the application. After this, you can perform the installation procedure for the current version of Kaspersky Industrial CyberSecurity for Networks.

After installing the current version of Kaspersky Industrial CyberSecurity for Networks, you can import the following data left over from the previous version into the new application:

- Security policies. You can import security policies that have been converted using the security policy conversion utility.
- Intrusion Detection rules. Use the rule replacement procedure for imports.

The database format of the current version of Kaspersky Industrial CyberSecurity for Networks is incompatible with the database format of the previous version of the application. For this reason, after the upgrade it will be impossible to load events that were registered in the previous version of the application. To save and view data on previously registered events, you can leave the Server of the previous version and install a Server of the up-to-date version on a different computer. If you do so, you will be able to connect to the Server of the previous version of the application to view previously registered events.

Removing the application

Kaspersky Industrial CyberSecurity for Networks is uninstalled by using the application installation script kics4net-deploy-<application version number>.bundle.sh. This script lets you remove 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 application removal, the script 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 installation script searches for a copy of the file on the computer and on other computers that have application components installed.

To remove individual nodes that perform functions of the Server or sensors:

1. Run the application installation script by completing steps 1–4 of the installation procedure.
2. In the menu for selecting the installation option, select **Edit settings of current installation**.

   The main 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 `SUDO password` invitations, enter the password for the user account that is used to perform the uninstallation.

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

To completely uninstall the application:

1. Run the application installation script by completing steps 1–4 of the installation procedure.

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

   The main 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 uninstallation. 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 component Network Agent, 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 `SUDO password` invitations, enter the password of the user performing the 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 additional files from the distribution kit that were manually copied to the computer (for example, the Kaspersky Industrial CyberSecurity for Networks API package). If necessary, these files can be manually deleted.

Starting and stopping the application

Application components installed on a computer are started automatically when the operating system of the computer is loaded.

> Kaspersky Industrial CyberSecurity for Networks receives industrial network traffic through monitoring points. After installation of Kaspersky Industrial CyberSecurity for Networks, there are no monitoring points on nodes that have application components installed. To perform industrial network control functions, you need to add monitoring points to nodes. If you need to pause the receipt and processing of traffic through a monitoring point, you can disable it.

To manage operation of the application and view information, you can connect to the Server through a web browser or start the Application Console.

Connecting to the Server through a web browser

You can use any supported web browser to connect to the Server through the web interface. The web browser must be installed on a 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 through a web browser:

1. Open the web browser.
2. Type the following in the address bar:
   ```
   https://<Server name>:<port>
   ```
   where:
   - `<Server name>` – IP address or computer name of the Server that was specified during installation of the Web Server.
   - `<port>` – port number that was specified during installation of the Web Server.

   > If the default port number (443) was specified during installation of 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.
3. On the account credentials entry page, enter the user name and password of the application user.
4. Click the **Log in** button.

   In the web browser window, you will see the Kaspersky Industrial CyberSecurity for Networks web interface page.

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.

Closing a Server connection session through a web browser

When you are done working with Kaspersky Industrial CyberSecurity for Networks through the web interface, perform the necessary actions to close the connection session in the web browser.

> If you close the web browser window without closing the connection session, the session remains active. An unclosed session remains active for up to 10 hours. During this time, the application can grant access to the Kaspersky Industrial CyberSecurity for Networks web interface without prompting for user account credentials, provided that the connection is used by the same computer, web browser, and operating system account.

To close the connection session with the Kaspersky Industrial CyberSecurity for Networks Server through a web browser:

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 **Log out**.

   The web browser window shows the page for entering account credentials.

Starting the Application Console

You can start the application Console on a computer that performs Server functions.

To start the Console, you must provide application user account credentials.

To start the Application Console:

1. In the applications start menu, select **Applications** → **System** → **Kaspersky Industrial CyberSecurity for Networks**.

   You will see a window for entering account credentials.
2. Enter the name and password of the application user.
3. Click the **Log in** button.

   The Application Console window appears on the screen.

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 Console session will terminate and the screen shows the window for entering account credentials. If this happens, to continue working you will need to re-enter your application user name and password.

Closing the application Console

You can terminate the Application Console at any time. This may be necessary, for example, to start the Console with the user name and password of a different application user.

After the Console closes, Kaspersky Industrial CyberSecurity for Networks Server continues running.

To close the Kaspersky Industrial CyberSecurity for Networks Console:

Close the Console window.

Application interface

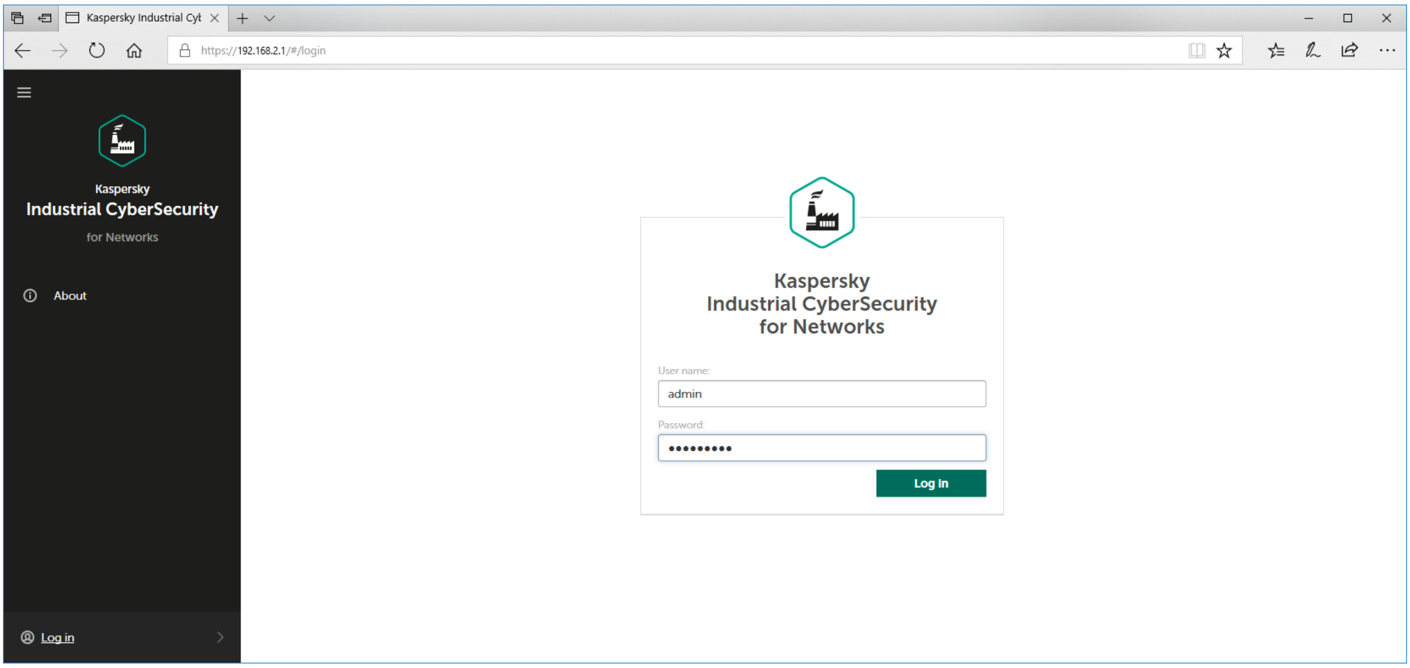
This section describes the primary application interface elements.

Web interface of Kaspersky Industrial CyberSecurity for Networks

This section provides a description of the application web interface.

Page for entering account credentials to connect through a web browser

To connect to the Kaspersky Industrial CyberSecurity for Networks Server, the page for entering account credentials opens in a web browser (see the figure below).



User name: admin

Password: •••••••••

Page for entering account credentials in a web browser window

The page contains fields for entering a user name and password, and the **Log in** button.

Menu of the Kaspersky Industrial CyberSecurity for Networks web interface

After connecting to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, the application web interface page opens.

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

After the user signs in, the menu contains the following elements:

- ≡ – expands and collapses the menu to increase free space on the page. If the menu is collapsed, only the images of elements are displayed within it.

- 🔔 – opens a list of notifications regarding application operating issues. If notifications are available, the notification status icon is displayed nearby.

- ⬇ – 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). If there are active background operations, the number and status of active operations is displayed nearby (green or red if there are operations with errors).

- Elements used for navigating to web interface sections:

  - ▦ – opens the Dashboard section.

  - 🖥 – opens the Assets section.

  - ▤ – opens the Network map section.

  - ⚠ – opens the Events section.

  - 🏷 – opens the Tags section.

  - 🌐 – opens the Network Control section.

  - ⚙ – opens the Settings section.

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

- ⚠ – displayed if some application functions are disabled or if learning mode is enabled for functions. If the menu is expanded, a message about disabled protection functions is displayed next to it. Clicking this icon or text opens a window containing information about disabled protection functions.

- 👤 – 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 and Console. These components use 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.

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

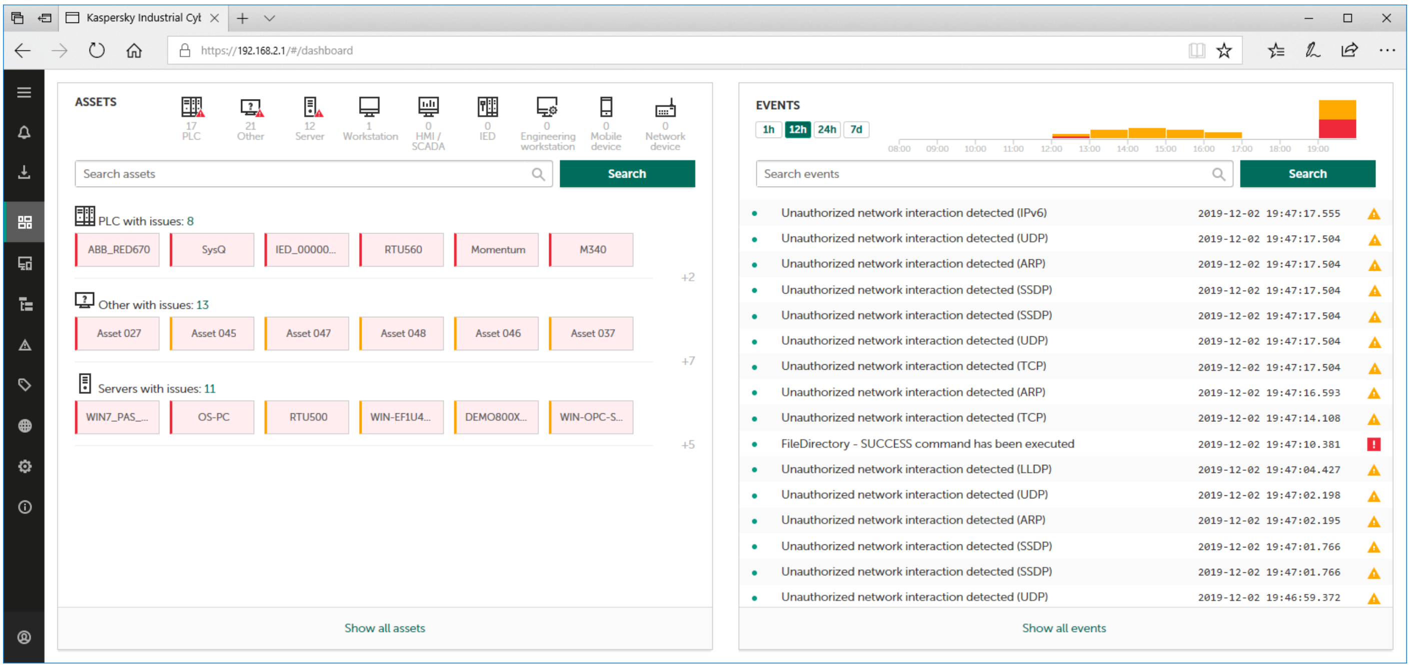
    - **Change password** – opens the window for changing the password of the current user.

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

    - **Help** – opens the Online Help page for Kaspersky Industrial CyberSecurity for Networks.

Dashboard section

In the **Dashboard** section of the application web interface (see the figure below), you can view the number of devices in the industrial network and information about the latest registered events and incidents in online mode.



PLC with issues: 8

ABB_RED670 | SysQ | IED_00000... | RTU560 | Momentum | M340 | +2

Other with issues: 13

Asset 027 | Asset 045 | Asset 047 | Asset 048 | Asset 046 | Asset 037 | +7

Servers with issues: 11

WIN7_PAS_... | OS-PC | RTU500 | WIN-EF1U4... | DEMO800X... | WIN-OPC-S... | +5

Unauthorized network interaction detected (IPv6)	2019-12-02 19:47:17.555	⚠
Unauthorized network interaction detected (UDP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (ARP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (SSDP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (SSDP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (UDP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (TCP)	2019-12-02 19:47:17.504	⚠
Unauthorized network interaction detected (ARP)	2019-12-02 19:47:16.593	⚠
Unauthorized network interaction detected (TCP)	2019-12-02 19:47:14.108	⚠
FileDirectory - SUCCESS command has been executed	2019-12-02 19:47:10.381	!
Unauthorized network interaction detected (LLDP)	2019-12-02 19:47:04.427	⚠
Unauthorized network interaction detected (UDP)	2019-12-02 19:47:02.198	⚠
Unauthorized network interaction detected (ARP)	2019-12-02 19:47:02.195	⚠
Unauthorized network interaction detected (SSDP)	2019-12-02 19:47:01.766	⚠
Unauthorized network interaction detected (SSDP)	2019-12-02 19:47:01.766	⚠
Unauthorized network interaction detected (UDP)	2019-12-02 19:46:59.372	⚠

Dashboard section

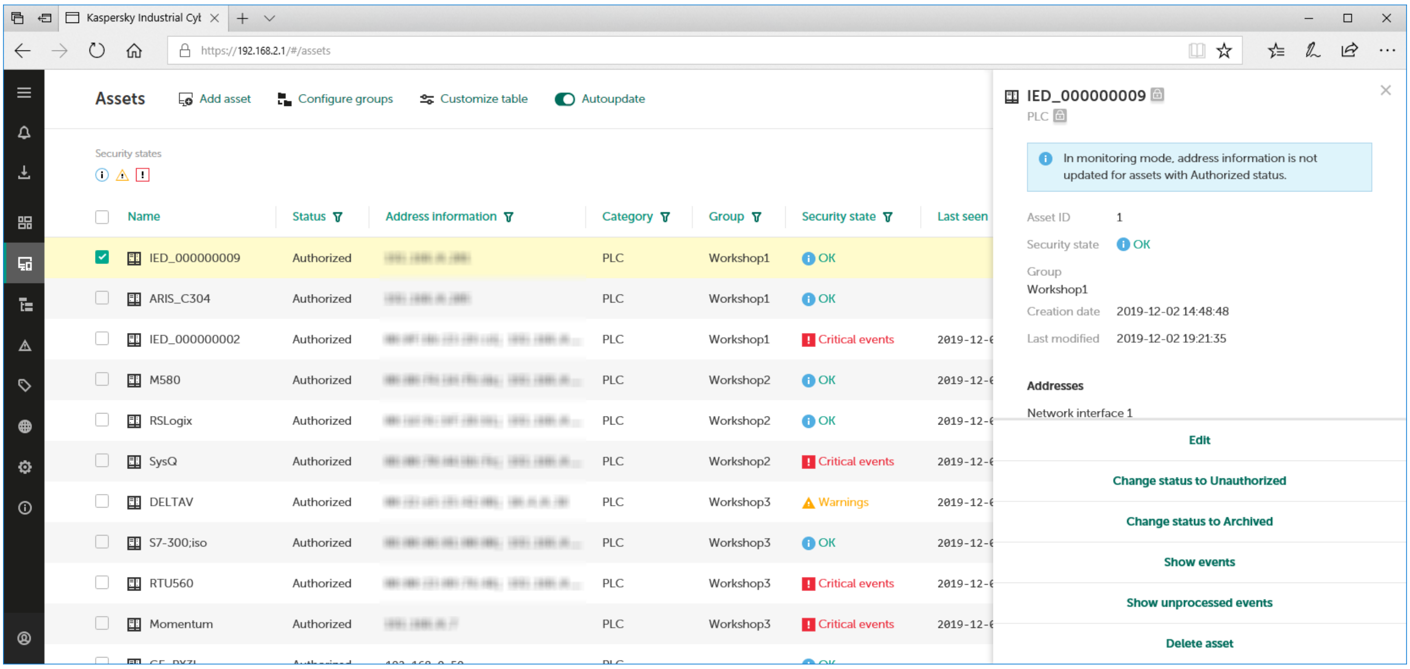
In the **Dashboard** section, information is provided in the following sections:

- **Assets** – contains information about devices. Devices are grouped by category.
- **Events** – contains information about the events and incidents that have the most recent values for the date and time of last occurrence.

The location of sections is fixed. The sections are automatically resized depending on the current size of the web browser window.

Assets section

In the **Assets** section of the application web interface (see the figure below), you can view and edit information about known assets.



Assets | Add asset | Configure groups | Customize table | Autoupdate

Security states

☐	Name	Status	Address information	Category	Group	Security state	Last seen
☑	IED_000000009	Authorized	[redacted]	PLC	Workshop1	OK	
☐	ARIS_C304	Authorized	[redacted]	PLC	Workshop1	OK	
☐	IED_000000002	Authorized	[redacted]	PLC	Workshop1	Critical events	2019-12-(
☐	M580	Authorized	[redacted]	PLC	Workshop2	OK	2019-12-(
☐	RSLogix	Authorized	[redacted]	PLC	Workshop2	OK	2019-12-(
☐	SysQ	Authorized	[redacted]	PLC	Workshop2	Critical events	2019-12-(
☐	DELTAV	Authorized	[redacted]	PLC	Workshop3	Warnings	2019-12-(
☐	S7-300;iso	Authorized	[redacted]	PLC	Workshop3	OK	2019-12-(
☐	RTU560	Authorized	[redacted]	PLC	Workshop3	Critical events	2019-12-(
☐	Momentum	Authorized	[redacted]	PLC	Workshop3	Critical events	2019-12-(

IED_000000009
PLC

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

Asset ID	1
Security state	OK
Group	Workshop1
Creation date	2019-12-02 14:48:48
Last modified	2019-12-02 19:21:35

Addresses

Network interface 1

Assets section

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

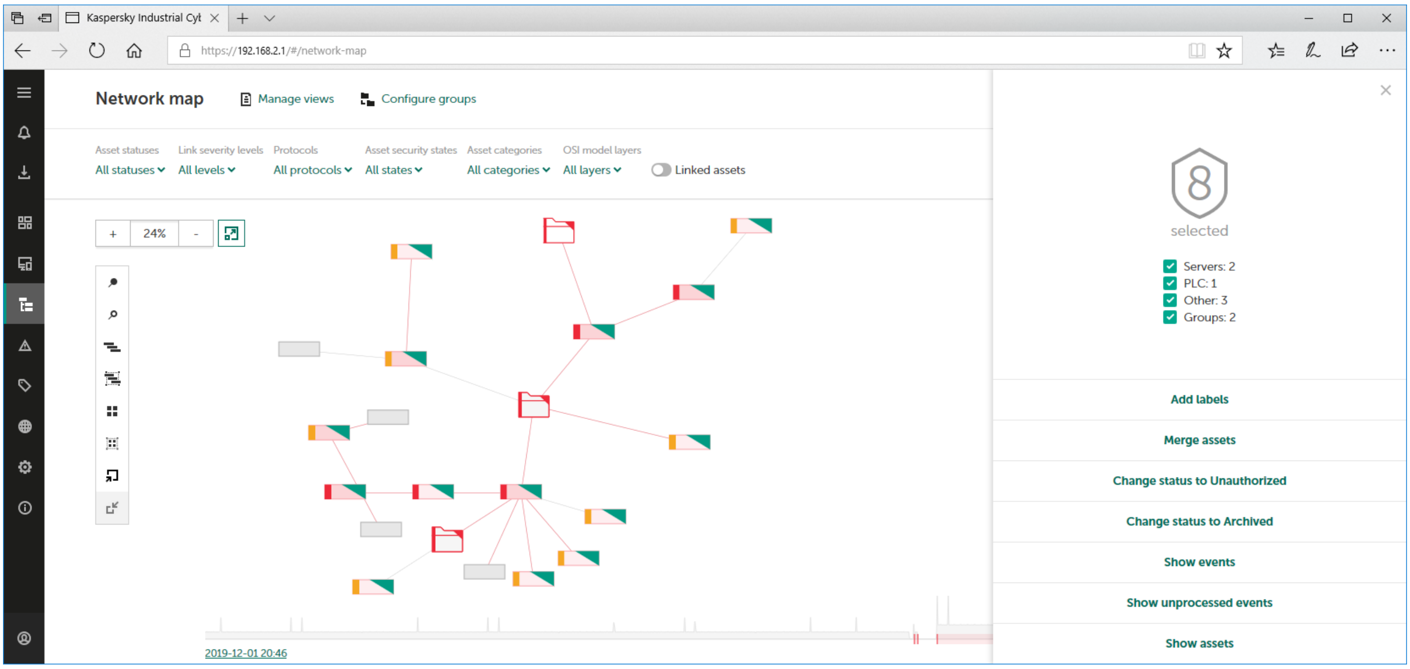
- **Add asset** – adds a new asset to the table.
- **Configure groups** – opens a window for creating an asset group tree. In this window, you can add or remove asset groups, arrange them in the tree, and rename them.
- **Customize table** – opens a window for configuring how the assets table is displayed. In this window, you can specify the columns to display and change the order in which they are displayed.
- **Autoupdate** – enables and disables automatic update of the assets table.
- Search field – lets you enter a query to search the assets table.
- **Security states** – groups buttons for selecting the option to filter assets by security state.
- **Clear filter** – resets the defined assets filter and search settings to their default state. The button is displayed if search or filter settings are defined.

The assets table is located in the main part of the **Assets** section. The table contains the columns specified during configuration of the displayed columns. You can sort and filter rules based on values in the columns.

When one or multiple assets are selected, the details area opens in the right part of the web interface window. This area contains information about the selected assets and the tools for managing them.

Network map section

In the **Network map** section of the application web interface (see the figure below), you can view information about the interactions of assets.



Network map section

The upper part of the **Network map** section has a toolbar containing the following management elements:

- **Manage views** – opens a window for saving and applying the network map display settings.
- **Configure groups** – opens a window for creating an asset group tree. In this window, you can add or remove asset groups, arrange them in the tree, and rename them.
- Search field – lets you enter a query to search nodes on the network map.
- **Asset statuses** – lets you configure filtering of nodes by asset status.
- **Link severity levels** – lets you configure filtering of links based on the severity of their associated events.
- **Protocols** – lets you configure filtering of links based on their communication protocols.
- **Asset states** – lets you configure filtering of nodes based on the security states of assets.
- **Asset categories** – lets you configure filtering of nodes by asset category.
- **OSI model layers** – lets you configure filtering of links based on the levels of communications corresponding to the layers of the OSI model (Open Systems Interconnection) for the network protocol stack.
- **Linked assets** – enables and disables the display of all nodes that have communicated with the filtered nodes (regardless of the defined filter settings).
- **Clear filter** – resets the defined object filter settings to their default state. This button is displayed if filter settings have been defined.

The network map display area shows nodes, links, and asset groups. The left part of the display area contains the following toolbars:

- Horizontal panel containing the + and – buttons for changing the scale, and the ⤢ button for automatic positioning of the network map.
- Vertical panel with the following buttons:

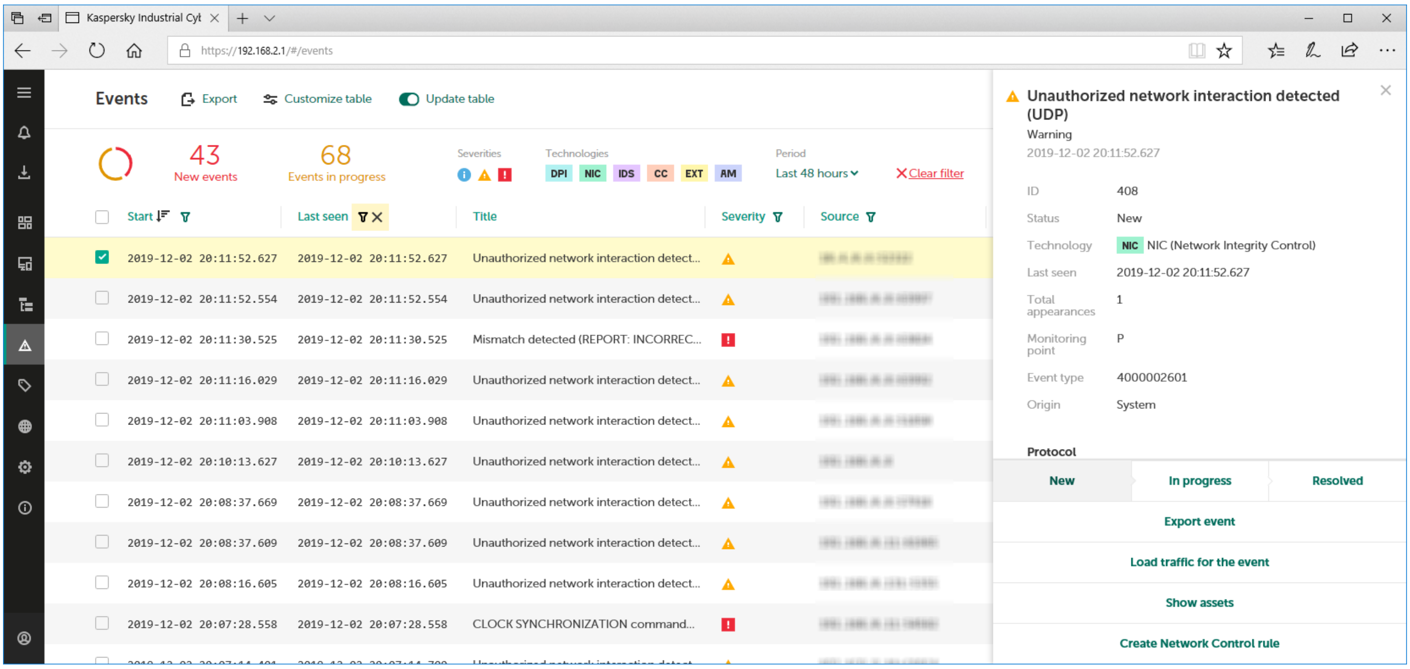
- – pins all the displayed nodes and collapsed groups.
- – unpins all the displayed nodes and collapsed groups.
- – radially arranges all nodes and collapsed groups.
- . – radially arranges the selected nodes and collapsed groups.
- – aligns all nodes and collapsed groups to the grid.
- – aligns the selected nodes and collapsed groups to the grid.
- – expands all the collapsed groups of assets.
- – collapses all the expanded groups of assets.

When one or multiple nodes or collapsed groups are selected, or when a link is selected, the details area opens in the right part of the web interface window. This area contains information about the selected objects and the tools for managing them.

The lower part of the **Network map** section contains a time scale that you can use to select the period for filtering nodes and links based on the time of their communications.

Events section

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



43 New events

68 Events in progress

	Start	Last seen	Title	Severity	Source
☑	2019-12-02 20:11:52.627	2019-12-02 20:11:52.627	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:11:52.554	2019-12-02 20:11:52.554	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:11:30.525	2019-12-02 20:11:30.525	Mismatch detected (REPORT: INCORREC...	!	[redacted]
□	2019-12-02 20:11:16.029	2019-12-02 20:11:16.029	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:11:03.908	2019-12-02 20:11:03.908	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:10:13.627	2019-12-02 20:10:13.627	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:08:37.669	2019-12-02 20:08:37.669	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:08:37.609	2019-12-02 20:08:37.609	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:08:16.605	2019-12-02 20:08:16.605	Unauthorized network interaction detect...	⚠	[redacted]
□	2019-12-02 20:07:28.558	2019-12-02 20:07:28.558	CLOCK SYNCHRONIZATION command...	!	[redacted]

Unauthorized network interaction detected (UDP)
Warning
2019-12-02 20:11:52.627

ID	408
Status	New
Technology	NIC NIC (Network Integrity Control)
Last seen	2019-12-02 20:11:52.627
Total appearances	1
Monitoring point	P
Event type	4000002601
Origin	System

Protocol

Events section

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

- **Export** – lets you export information about all events and incidents with respect to the current filter and search settings in the events table.

- **Customize table** – opens a window for configuring how the events table is displayed. In this window, you can enable or disable the display of the information panel, select the display mode for events and incidents, and specify the displayed columns and change the order in which they are displayed.

- **Update table** – enables and disables automatic update of the events table. Automatic update is enabled by default. When automatic update is enabled, the table of registered events is updated in online mode. In this case, the table is sorted by the **Last seen** column in descending order of the dates and times when the conditions for event registration occurred. If you choose to sort by another column, the events table will no longer be updated.

- Search field – lets you enter a query to search for events and incidents in the table.

- Information panel – contains a chart showing the ratio between events with the *New* status and events with the *In progress* status. On the right of the chart is the number of events with these statuses in the database. You can enable and disable the display of the information panel in the window that lets you configure the display of the events table.

- **Severity** – groups buttons for enabling and disabling the filtering of events and incidents based on their importance level: *Informational* ⓘ, *Warning* ⚠ and *Critical* ❗.

- **Technologies** – groups buttons for enabling and disabling event filtering based on technology: *Deep Packet Inspection* (DPI), *Network Integrity Control* (NIC), *Intrusion Detection* (IDS), *Command Control* (CC), *External* (EXT) and *Asset Management* (AM).

- **Period** – lets you filter events and incidents by time period. You can select one of four standard periods or manually specify a period using the **Specify a period** option. When manually configuring the period, you will see additional fields for selecting the date and time of the beginning and end of the period. If you manually specify a period, the table will no longer be updated.

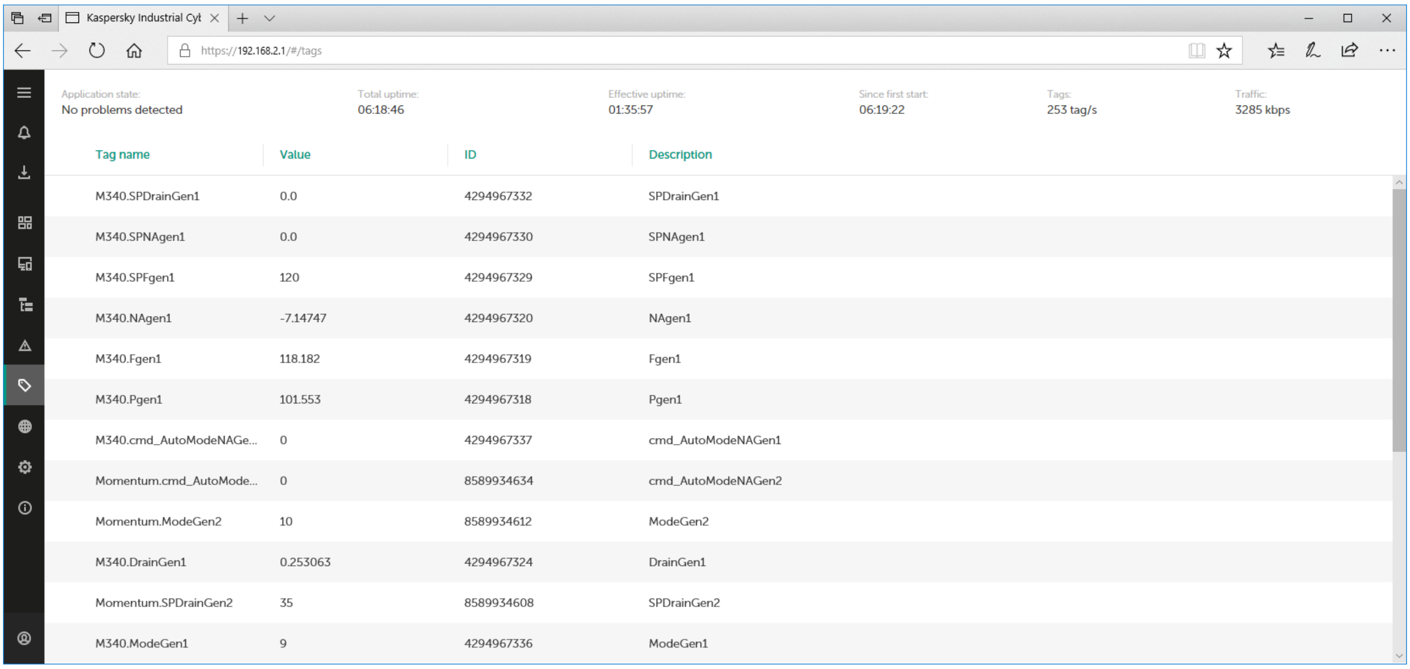
- **Clear filter** – resets the defined events filter and search settings to their default state. The button is displayed if search or filter settings are defined.

The main part of the **Events** section shows a table containing information about registered events and incidents. The information is presented in the columns configured to be displayed. You can sort and filter events and incidents based on values in the columns.

When events or incidents are selected, the details area opens in the right part of the web interface window. This area contains information about the selected events and incidents and the tools for managing them.

Tags section

In the **Tags** section of the application web interface (see the figure below), you can view tags with process parameter values and monitor the current state of Kaspersky Industrial CyberSecurity for Networks.



Application state:
No problems detected

Total uptime:
06:18:46

Effective uptime:
01:35:57

Since first start:
06:19:22

Tags:
253 tag/s

Traffic:
3285 kbps

Tag name	Value	ID	Description
M340.SPDrainGen1	0.0	4294967332	SPDrainGen1
M340.SPNAgen1	0.0	4294967330	SPNAgen1
M340.SPFgen1	120	4294967329	SPFgen1
M340.NAgen1	-7.14747	4294967320	NAgen1
M340.Fgen1	118.182	4294967319	Fgen1
M340.Pgen1	101.553	4294967318	Pgen1
M340.cmd_AutoModeNAGe...	0	4294967337	cmd_AutoModeNAGen1
Momentum.cmd_AutoMode...	0	8589934634	cmd_AutoModeNAGen2
Momentum.ModeGen2	10	8589934612	ModeGen2
M340.DrainGen1	0.253063	4294967324	DrainGen1
Momentum.SPDrainGen2	35	8589934608	SPDrainGen2
M340.ModeGen1	9	4294967336	ModeGen1

Tags section

The following information about the current state of Kaspersky Industrial CyberSecurity for Networks is displayed in the upper part of the **Tags** section:

- **Application state** – current operating state of the application. The following application state information may be displayed: *No problems detected*, *An error occurred*, and *Unknown*.
- **Total uptime** – application operating time that has elapsed since the first startup of Kaspersky Industrial CyberSecurity for Networks until the current time. It includes periods of normal operation of the application (without incidents) and periods when the operation of the application was disrupted.
- **Effective uptime** – duration of normal operation of the application (without incidents) since the most recent launch of Kaspersky Industrial CyberSecurity for Networks until present.
- **Since first start** – application operating time that has elapsed since the first startup of Kaspersky Industrial CyberSecurity for Networks. It includes periods of normal operation (without incidents), periods when operation was disrupted, and periods when the Kaspersky Industrial CyberSecurity for Networks Server was shut down.
- **Tags** – tag processing rate (tags/s).
- **Traffic** – incoming traffic rate (kbps).

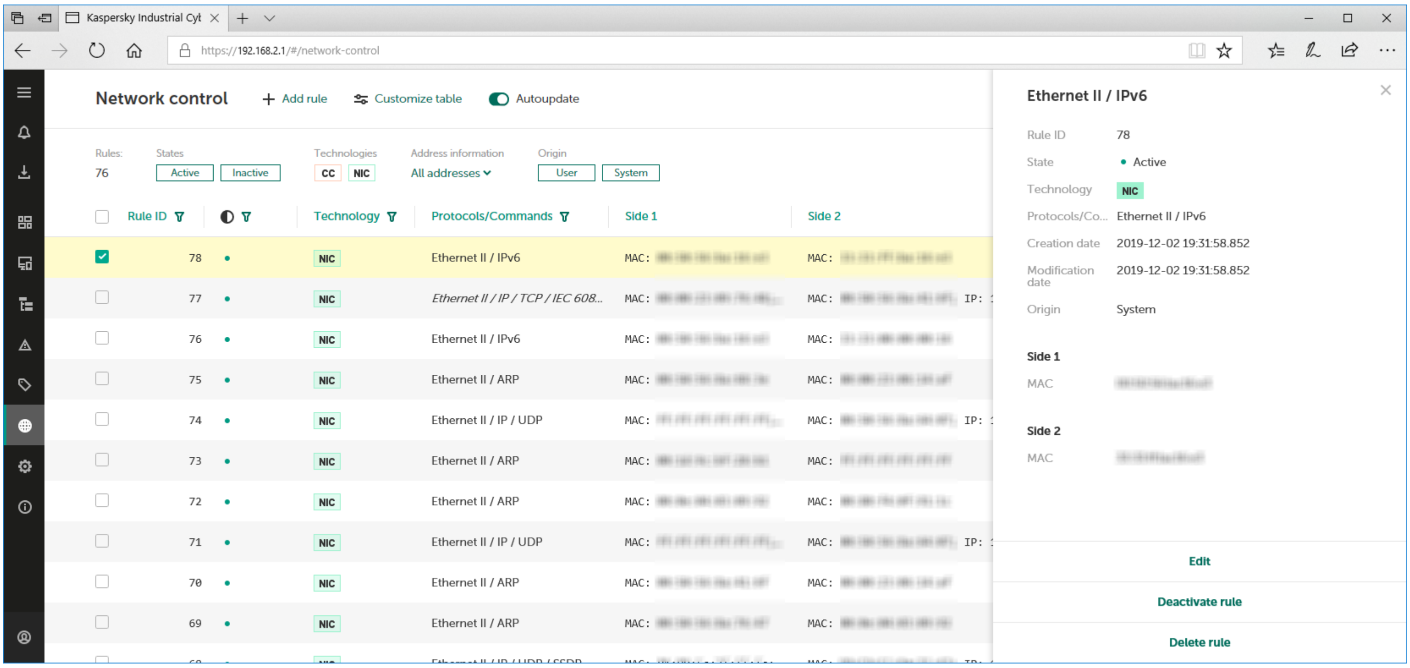
The table of process parameters contains the tags that are specified in Process Control rules. The columns in the table contain the following information about tags:

- **Tag name** – tag name defined in the list of devices and tags.
- **Value** – current value of the tag.
- **ID** – numerical ID of the tag. It is assigned when a tag is added to the list of devices and tags.
- **Description** – brief description of a tag defined in the list of devices and tags.

You can sort tags based on the values in columns, except for the **Value** column.

Network Control section

In the **Network Control** section of the application web interface (see the figure below), you can manage Network Control rules.



Kaspersky Industrial Cyt

https://192.168.2.1/#/network-control

Network control + Add rule · Customize table · Autoupdate

Rules: 76 · States: Active, Inactive · Technologies: CC, NIC · Address information: All addresses · Origin: User, System

☐	Rule ID	◐	Technology	Protocols/Commands	Side 1	Side 2
☑	78	●	NIC	Ethernet II / IPv6	MAC: [redacted]	MAC: [redacted]
☐	77	●	NIC	*Ethernet II / IP / TCP / IEC 608...*	MAC: [redacted]	MAC: [redacted] IP:
☐	76	●	NIC	Ethernet II / IPv6	MAC: [redacted]	MAC: [redacted]
☐	75	●	NIC	Ethernet II / ARP	MAC: [redacted]	MAC: [redacted]
☐	74	●	NIC	Ethernet II / IP / UDP	MAC: [redacted]	MAC: [redacted] IP:
☐	73	●	NIC	Ethernet II / ARP	MAC: [redacted]	MAC: [redacted]
☐	72	●	NIC	Ethernet II / ARP	MAC: [redacted]	MAC: [redacted]
☐	71	●	NIC	Ethernet II / IP / UDP	MAC: [redacted]	MAC: [redacted] IP:
☐	70	●	NIC	Ethernet II / ARP	MAC: [redacted]	MAC: [redacted]
☐	69	●	NIC	Ethernet II / ARP	MAC: [redacted]	MAC: [redacted]

Ethernet II / IPv6

Rule ID	78
State	● Active
Technology	NIC
Protocols/Co...	Ethernet II / IPv6
Creation date	2019-12-02 19:31:58.852
Modification date	2019-12-02 19:31:58.852
Origin	System

Side 1

MAC [redacted]

Side 2

MAC [redacted]

Network Control section

The upper part of the **Network Control** section has a toolbar containing the following elements for managing the table of Network Control rules:

- **Add rule** – creates a new Network Control rule.
- **Customize table** – opens a window for configuring how the Network Control rules table is displayed. In this window, you can specify the columns to display and change the order in which they are displayed.
- **Autoupdate** – enables and disables automatic update of the rules table.
- **Refresh** – appears in the upper part of the **Network Control** section if autoupdate of the rules table is disabled.
- Search field – lets you enter a query to search the rules table.
- **Rules** – displays the total number of Network Control rules (including rules that are not currently displayed).
- **States** – groups buttons for filtering rules by state.
- **Technologies** – groups buttons for filtering rules by technology: *Command Control* (CC) and *Network Integrity Control* (NIC).
- **Address information** – lets you configure filtering of rules based on the address information contained in the rules.
- **Origin** – groups buttons for filtering rules by origin.

- **Clear filter** – resets the defined rules filter and search settings to their default state. The button is displayed if search or filter settings are defined.

The network control rules table is located in the main part of the **Network Control** section. The table contains the columns specified during configuration of the displayed columns. You can sort and filter rules based on values in the columns.

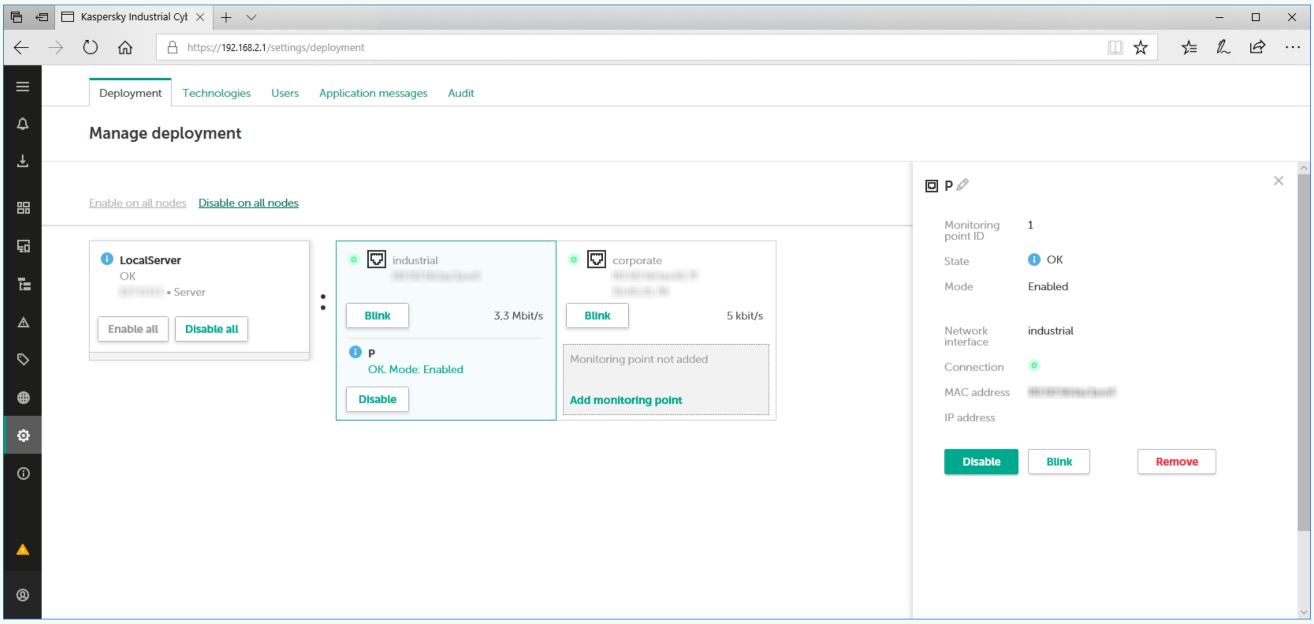
When one or multiple rules are selected, the details area opens in the right part of the web interface window. This area contains information about the selected rules and the tools for managing them.

Settings section

The **Settings** section of the application web interface may contain the following tabs:

- Deployment ?

On the **Deployment** tab in the **Settings** section (see the figure below), you can view information about nodes that have application components installed, and about network interfaces and monitoring points on nodes. If a user account with the Administrator role was used to connect to the Server, you can also manage monitoring points on this tab.



Manage deployment

LocalServer
OK
• Server

industrial
3,3 Mbit/s
P
OK. Mode: Enabled

corporate
5 kbit/s
Monitoring point not added

P

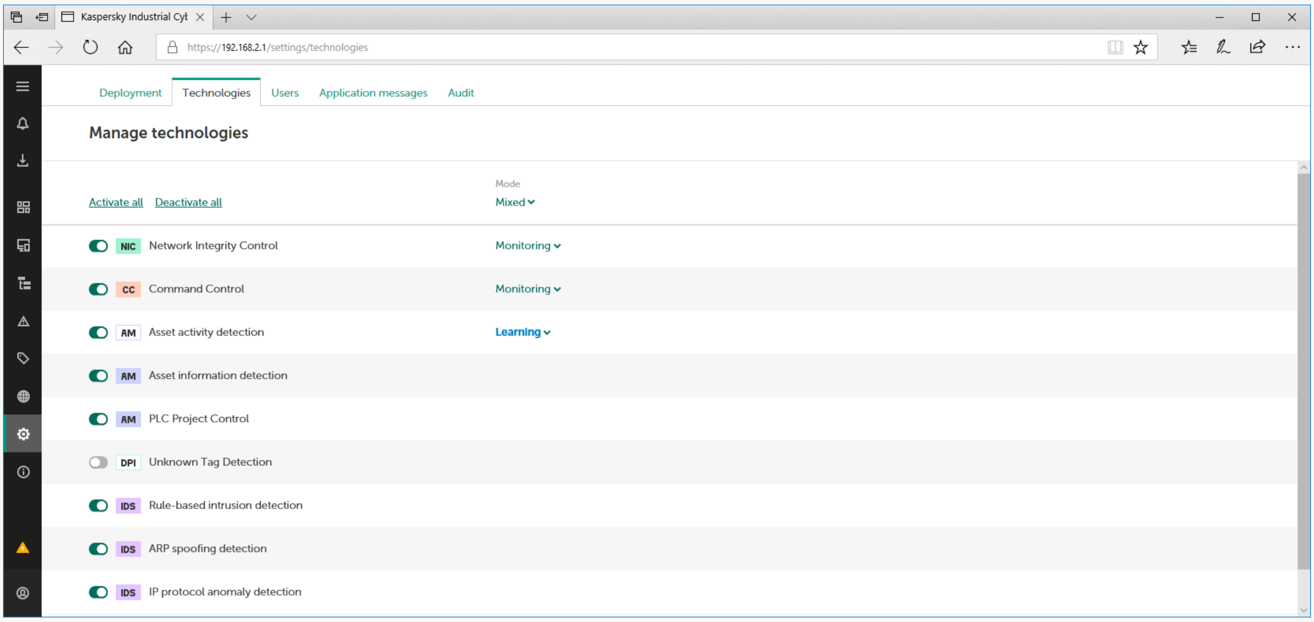
Monitoring point ID: 1
State: OK
Mode: Enabled
Network interface: industrial
Connection
MAC address
IP address

Settings section. **Deployment** tab

The **Deployment** tab contains the tiles of nodes that have application components installed (on the left) and tiles of the network interfaces on these nodes (on the right of each node). When you select a node tile or network interface tile, the details area appears in the right part of the window.

- Technologies ?

On the **Technologies** tab in the **Settings** section (see the figure below), you can manage the technologies and methods used for analyzing traffic in Kaspersky Industrial CyberSecurity for Networks. The **Technologies** tab is displayed if a user account with the Administrator role was used to connect to the Server.



Manage technologies

Activate all Deactivate all

Mode
Mixed

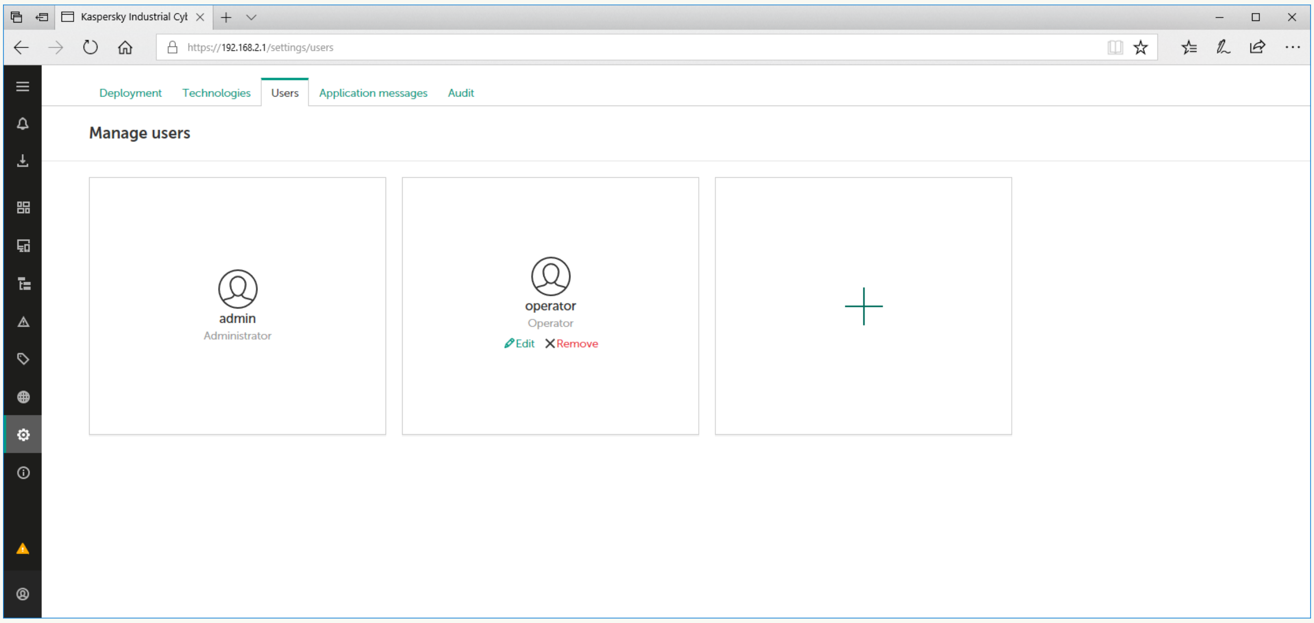
NIC	Network Integrity Control	Monitoring
CC	Command Control	Monitoring
AM	Asset activity detection	Learning
AM	Asset information detection	
AM	PLC Project Control	
DPI	Unknown Tag Detection	
IDS	Rule-based intrusion detection	
IDS	ARP spoofing detection	
IDS	IP protocol anomaly detection	

Settings section. Technologies tab

The **Technologies** tab contains a list of technologies and methods for which you can change the states and operating modes.

- Users

On the **Users** tab in the **Settings** section (see the figure below), you can manage application user accounts. The **Users** tab is displayed if a user account with the Administrator role was used to connect to the Server.



Manage users

admin
Administrator

operator
Operator
Edit Remove

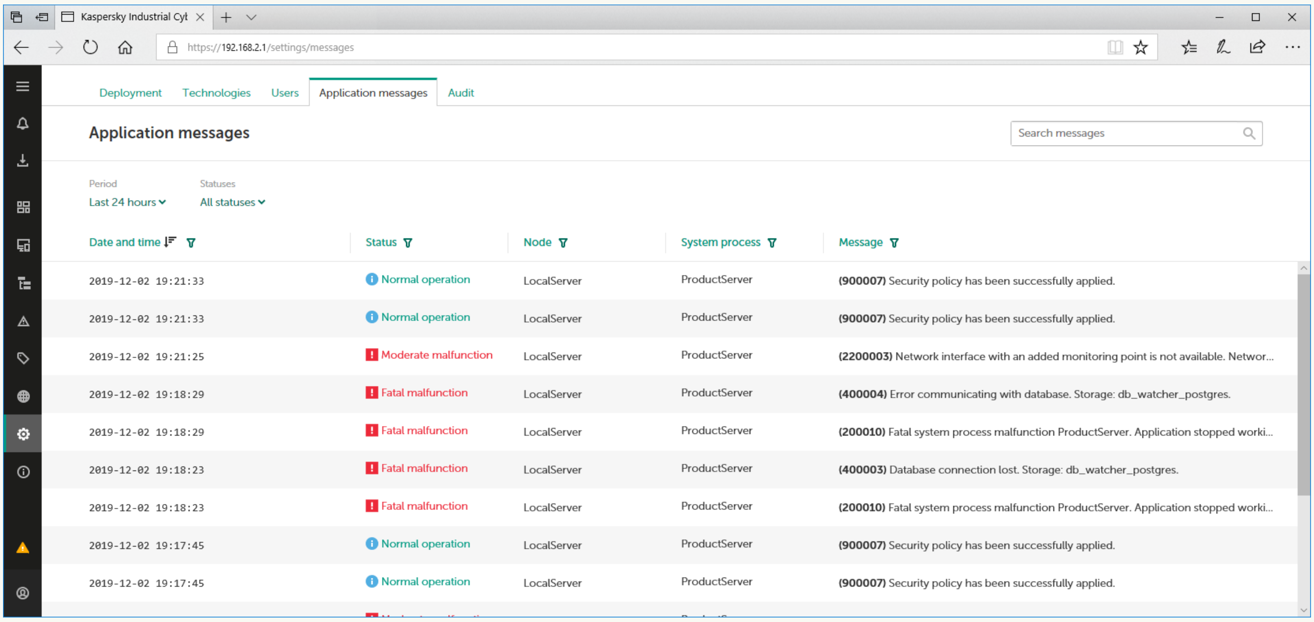
+

Settings section. Users tab

The **Users** tab contains tiles for application users and a tile with the plus (+) icon for adding user accounts.

- Application messages

On the **Application messages** tab in the **Settings** section (see the figure below), you can view messages about application operation.



Application messages

Period: Last 24 hours

Statuses: All statuses

Date and time	Status	Node	System process	Message
2019-12-02 19:21:33	Normal operation	LocalServer	ProductServer	**(900007)** Security policy has been successfully applied.
2019-12-02 19:21:33	Normal operation	LocalServer	ProductServer	**(900007)** Security policy has been successfully applied.
2019-12-02 19:21:25	Moderate malfunction	LocalServer	ProductServer	**(2200003)** Network interface with an added monitoring point is not available. Networ...
2019-12-02 19:18:29	Fatal malfunction	LocalServer	ProductServer	**(400004)** Error communicating with database. Storage: db_watcher_postgres.
2019-12-02 19:18:29	Fatal malfunction	LocalServer	ProductServer	**(200010)** Fatal system process malfunction ProductServer. Application stopped worki...
2019-12-02 19:18:23	Fatal malfunction	LocalServer	ProductServer	**(400003)** Database connection lost. Storage: db_watcher_postgres.
2019-12-02 19:18:23	Fatal malfunction	LocalServer	ProductServer	**(200010)** Fatal system process malfunction ProductServer. Application stopped worki...
2019-12-02 19:17:45	Normal operation	LocalServer	ProductServer	**(900007)** Security policy has been successfully applied.
2019-12-02 19:17:45	Normal operation	LocalServer	ProductServer	**(900007)** Security policy has been successfully applied.

Settings section. **Application messages** tab

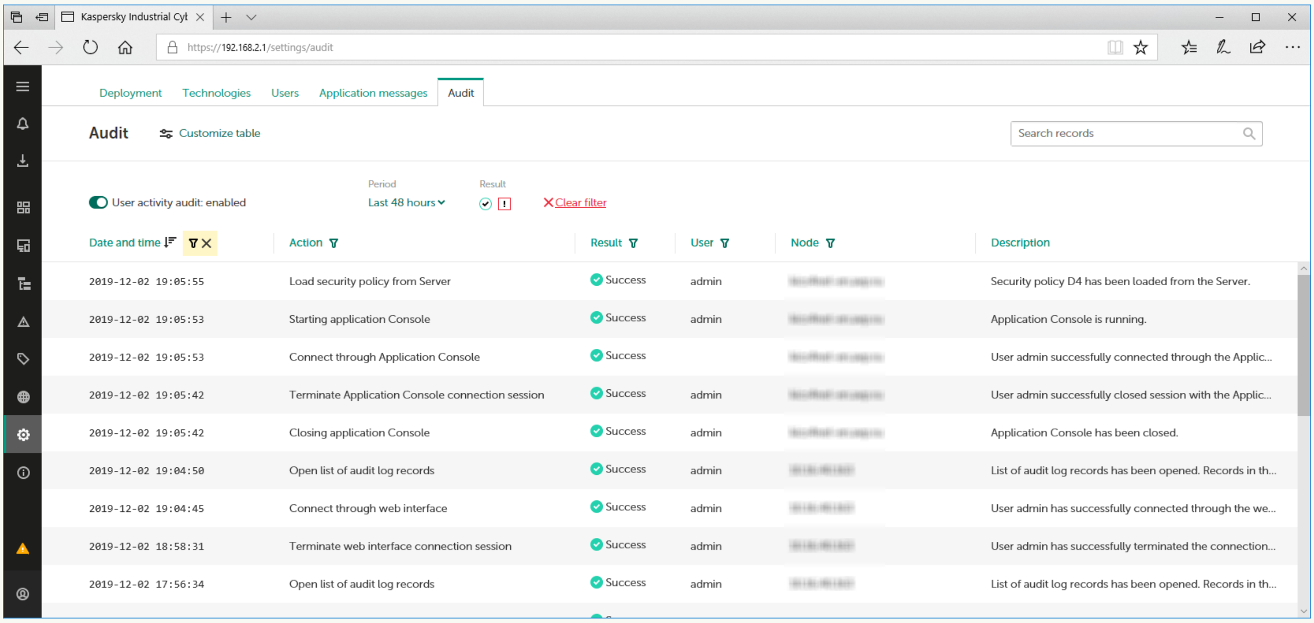
The upper part of the **Application messages** tab has a toolbar containing the following management elements:

- Search field – lets you enter a query to search messages in the table.
- **Period** – lets you filter application messages by time period. You can select one of four standard periods or manually specify a period using the **Specify a period** option. When manually configuring the period, you will see additional fields for selecting the date and time of the beginning and end of the period. If you manually specify a period, the table will no longer be updated.
- **Statuses** – lets you configure filtering of messages based on their statuses.
- **Clear filter** – resets the defined message filter and search settings to their default state. The button is displayed if search or filter settings are defined.

Below is a table containing information about registered application messages. You can sort and filter messages based on values in the table columns.

- Audit

On the **Audit** tab in the **Settings** section (see the figure below), you can view audit log entries and enable or disable the user activity audit. The **Audit** tab is displayed if a user account with the Administrator role was used to connect to the Server.



Date and time	Action	Result	User	Node	Description
2019-12-02 19:05:55	Load security policy from Server	✓ Success	admin	[redacted]	Security policy D4 has been loaded from the Server.
2019-12-02 19:05:53	Starting application Console	✓ Success	admin	[redacted]	Application Console is running.
2019-12-02 19:05:53	Connect through Application Console	✓ Success		[redacted]	User admin successfully connected through the Applic...
2019-12-02 19:05:42	Terminate Application Console connection session	✓ Success	admin	[redacted]	User admin successfully closed session with the Applic...
2019-12-02 19:05:42	Closing application Console	✓ Success	admin	[redacted]	Application Console has been closed.
2019-12-02 19:04:50	Open list of audit log records	✓ Success	admin	[redacted]	List of audit log records has been opened. Records in th...
2019-12-02 19:04:45	Connect through web interface	✓ Success	admin	[redacted]	User admin has successfully connected through the we...
2019-12-02 18:58:31	Terminate web interface connection session	✓ Success	admin	[redacted]	User admin has successfully terminated the connection...
2019-12-02 17:56:34	Open list of audit log records	✓ Success	admin	[redacted]	List of audit log records has been opened. Records in th...

Settings section. **Audit** tab

The upper part of the **Audit** tab has a toolbar containing the following management elements:

- **Customize table** – opens a window for configuring how the audit entries table is displayed. In this window, you can specify the columns to display and change the order in which they are displayed.
- Search field – lets you enter a query to search entries in the table.
- **User activity audit: enabled / disabled** – enables or disables the user activity audit.
- **Period** – lets you filter audit entries by time period. You can select one of four standard periods or manually specify a period using the **Specify a period** option. When manually configuring the period, you will see additional fields for selecting the date and time of the beginning and end of the period. If you manually specify a period, the table will no longer be updated.
- **Result** – groups buttons for enabling and disabling audit entry filtering based on the results of actions: *Success* ✓ and *Failure* ❗.
- **Clear filter** – resets the defined entries filter and search settings to their default state. The button is displayed if search or filter settings are defined.

Below is a table containing information about registered audit entries. You can sort and filter entries based on values in the table columns.

The displayed tabs depend on which role is assigned to the user who established the connection to the Server.

Kaspersky Industrial CyberSecurity for Networks Console

This section provides a description of Application Console interface elements.

Elements of the Kaspersky Industrial CyberSecurity for Networks Console interface

The window of the Kaspersky Industrial CyberSecurity for Networks Console contains a title, main menu, tab display area, and application state bar.

The title of the Console window displays the application name and the name of the security policy that is open in the Console. The security policy name is enclosed in square brackets. If changes to the security policy have not been saved, the security policy name is marked with the * character.

Under the title of the Console window is the application's main menu, which contains the following items:

- **Manage security policy** – groups menu items used for performing actions with security policies of Kaspersky Industrial CyberSecurity for Networks:
  - **Create** – creates a new security policy.
  - **Open** – opens a saved security policy from the selected folder.
  - **Save** – saves changes to the current security policy (if you are saving it for the first time, you will see a window for selecting the folder to save it in).
  - **Save as** – lets you save the security policy in the selected folder (you will see a window for selecting the folder to save it in).
  - **Apply** – applies the current security policy on the Server.
  - **Load from Server** – loads the security policy that is applied on the Server in the Console.
  - **Properties** – opens a window containing information about the security policy that is currently open in the Console and information about the security policy that is running on the Server.
  - **Recent** – contains items that let you quickly open one of the security policies that was recently opened in the Console (each menu item contains a security policy name and path to the folder containing the security policy files).
- **Settings** – groups menu items used for opening management and configuration windows:
  - **Server and sensors** – opens a window for viewing general information about nodes that have application components installed and for changing the log levels for application process logs.
  - **Logs** – opens a window in which you can edit the settings for storing entries in application logs, and edit the settings for storing traffic saved during event registration.
  - **Update** – opens a window for configuring settings and starting an update.
- **Help** – groups the following menu items:
  - **License key** – opens a window for viewing information about the update license key, and also provides the capability to add or remove the license key.
  - **About** – opens a window containing brief information about the application.

The following tabs are located in the tab display area:

- Process control
- Configure events
- Intrusion detection

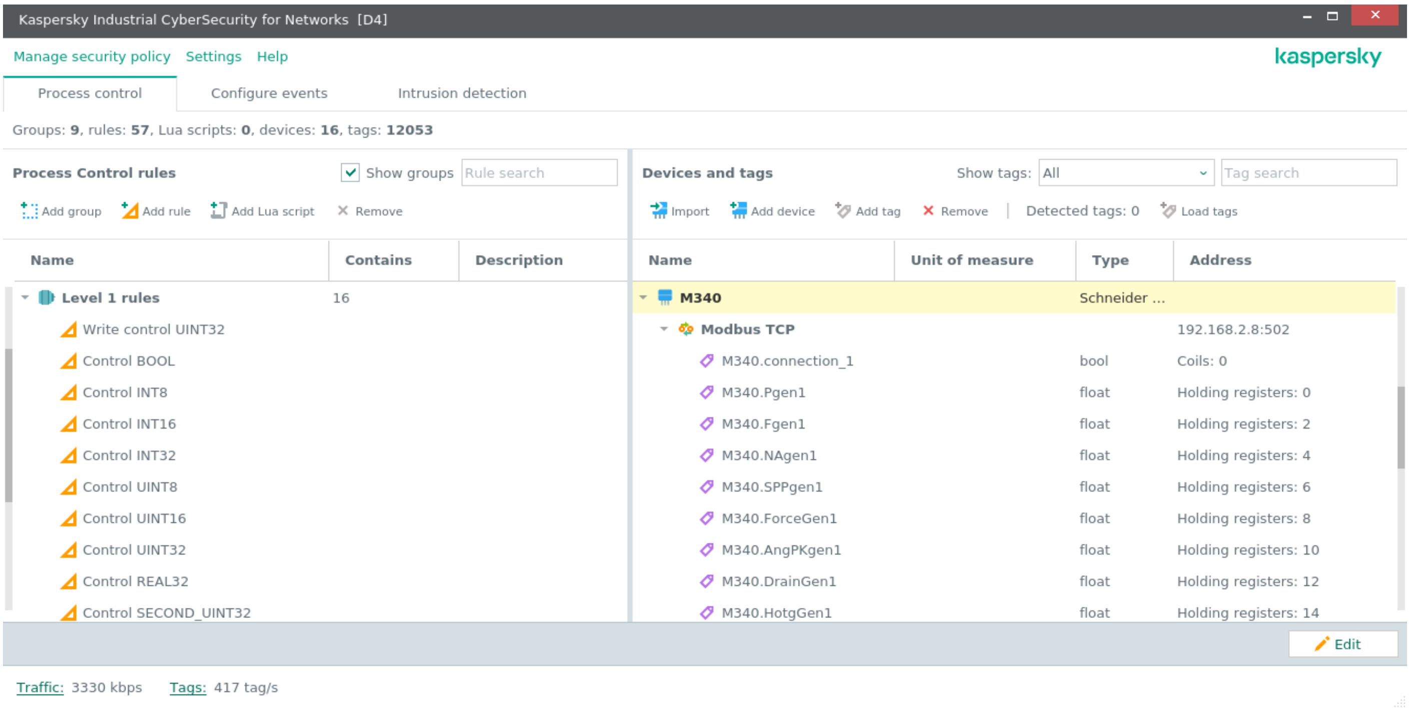
The status bar of Kaspersky Industrial CyberSecurity for Networks is located in the lower part of the Console window. The status bar displays the following information:

- **Traffic** reflects the flow of traffic within the controlled network. The unit of measure is kbps.

- **Tags** – shows the stream of tags. The unit of measure is tag per second.
- Information about the application state when there are application operating issues.
- Information about the license key when there are key status warnings.

Process control tab

In the Application Console on the **Process control** tab (see the figure below), you can configure Process Control rules and form a hierarchical structure of process control devices, monitored protocols and tags.



Groups: **9**, rules: **57**, Lua scripts: **0**, devices: **16**, tags: **12053**

Name	Contains	Description
Level 1 rules	16	
Write control UINT32		
Control BOOL		
Control INT8		
Control INT16		
Control INT32		
Control UINT8		
Control UINT16		
Control UINT32		
Control REAL32		
Control SECOND_UINT32		

Detected tags: 0

Name	Unit of measure	Type	Address
M340		Schneider ...	
Modbus TCP			192.168.2.8:502
M340.connection_1		bool	Coils: 0
M340.Pgen1		float	Holding registers: 0
M340.Fgen1		float	Holding registers: 2
M340.NAgen1		float	Holding registers: 4
M340.SPPgen1		float	Holding registers: 6
M340.ForceGen1		float	Holding registers: 8
M340.AngPKgen1		float	Holding registers: 10
M340.DrainGen1		float	Holding registers: 12
M340.HotgGen1		float	Holding registers: 14

Traffic: 3330 kbps Tags: 417 tag/s

Process control tab

The upper part of the tab contains a bar with information about Process Control settings. The bar indicates the number of rules, rule groups, Lua scripts, devices, and tags.

The **Process control** tab displays two tables: the **Process Control rules** table is displayed on the left, and the **Devices and tags** table is displayed on the right. Toolbars containing buttons for managing lists are located above the tables.

Process Control rules

The table of Process Control rules contains the rules describing the conditions for registering events in Kaspersky Industrial CyberSecurity for Networks. You can logically combine rules into groups.

Above the table of Process Control rules is a toolbar containing the following control elements:

- **Show groups** – enables or disables the display of groups.
- Search field – lets you enter a query to search for rules based on the values in displayed columns of the rules table.
- **Add group** – adds a group.

- **Add rule** – adds a Process Control rule with settings of conditions.
- **Add Lua script** – adds a Process Control rule with a Lua script.
- **Remove** – removes the selected rule or group.

The table of Process Control rules contains the following columns:

- **Name** – displays the name of the rule or group.
- **Contains** – displays the number of items (groups, rules, and Lua scripts) belonging to the group.
- **Description** – displays brief description of the rule.

You can change the width of columns and switch the places of the **Contains** and **Description** columns.

Devices and tags

The table of devices and tags displays the relationship between process items: process control devices, protocols, and tags. A tree structure is used to represent the items.

Above the table of devices and tags is a toolbar containing the following control elements:

- **Show tags** – lets you select a tag display option in the drop-down list:
  - **All** – the table contains all tags created in the current security policy.
  - **In rules** – the table contains tags used in any rules in the current security policy.
  - **In the current rule** – the table contains tags used in the selected Process Control rule.
- Search field – lets you enter a query to search for tags based on the values in the displayed columns of the table of devices and tags, and based on tag IDs. To search by tag ID, you need to enter `id:` in the search string and specify the relevant IDs separated by a space (for example, `id: 3 52 675`).
- **Import** – imports tags and process control devices from data files.
- **Add device** – adds a process control device.
- **Add tag** – adds a tag for the selected device and protocol.
- **Remove** – removes the selected device or tag.
- **Detected tags** – displays the number of tags in the detected tag storage.
- **Load tags** – loads tags from the detected tag storage.

The table of devices and tags contains the following columns:

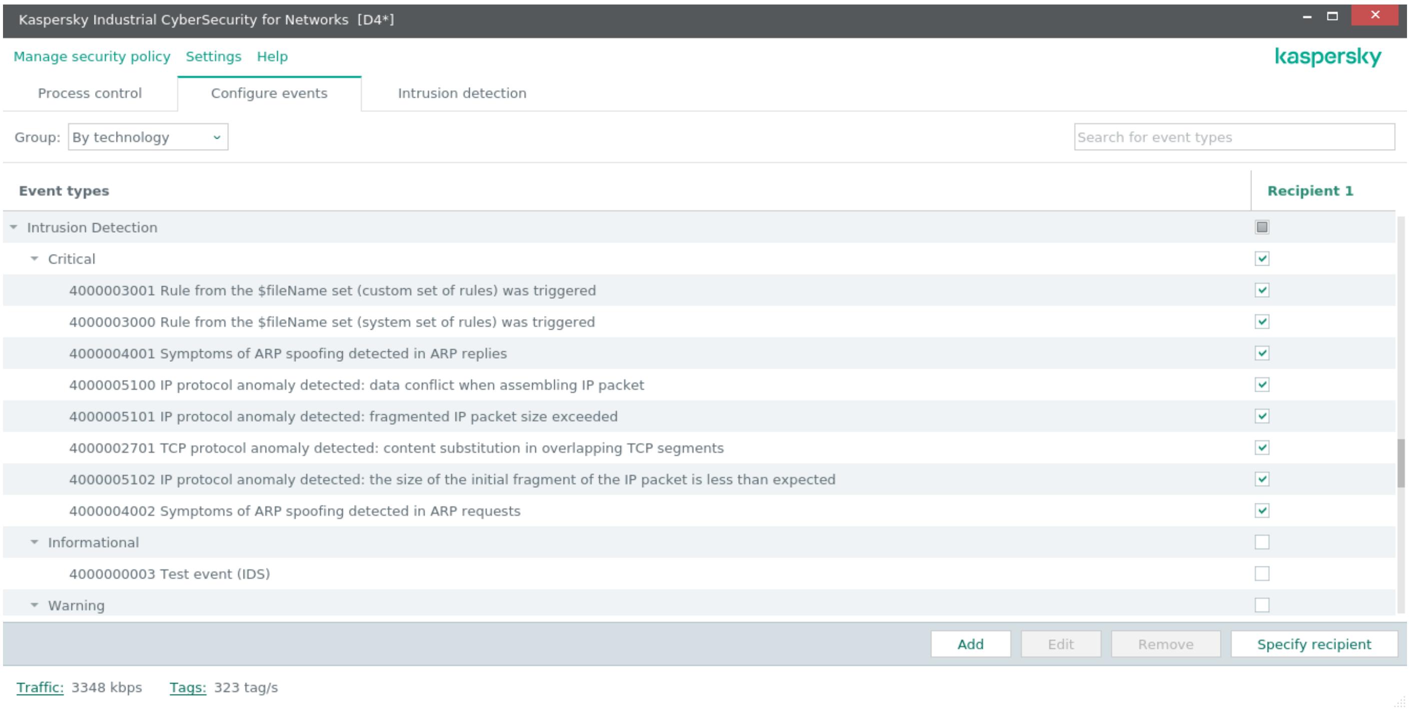
- **Name** – displays the name of the list item.
- **Unit of measure** – displays the unit of measure of the tag value.
- **Type** – displays the type of process control device or tag.

- **Address** – displays address information. For protocols, the IP address, port, and MAC address of the process control device are specified. For tags, the physical address of the tag in device memory is specified.

You can change the width of columns, and change the places of the **Unit of measure**, **Type** and **Address** columns.

Configure events tab

On the **Configure events** tab (see the figure below), you can configure the event types of Kaspersky Industrial CyberSecurity for Networks and configure the transmission of events to recipient systems. The *event type* is the displayed text of the event containing variables without including the specific values of the settings. The settings values are provided by the Server when an event is generated. Events of the same type may have different settings values (for example, tags and protocols), but they have the same set of settings and event description text.



Event types	Recipient 1
Intrusion Detection	■
Critical	☑
4000003001 Rule from the $fileName set (custom set of rules) was triggered	☑
4000003000 Rule from the $fileName set (system set of rules) was triggered	☑
4000004001 Symptoms of ARP spoofing detected in ARP replies	☑
4000005100 IP protocol anomaly detected: data conflict when assembling IP packet	☑
4000005101 IP protocol anomaly detected: fragmented IP packet size exceeded	☑
4000002701 TCP protocol anomaly detected: content substitution in overlapping TCP segments	☑
4000005102 IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	☑
4000004002 Symptoms of ARP spoofing detected in ARP requests	☑
Informational	☐
4000000003 Test event (IDS)	☐
Warning	☐

Traffic: 3348 kbps Tags: 323 tag/s

Configure events tab

Above the **Event types** list is a toolbar containing the following control elements:

- **Group** – lets you select the method used to group event types in the drop-down list: **By technology**, **By severity** or **Do not group**.

- Search field – lets you enter a search query in the list of event types.

The list of **Event types** contains the numbers and titles of event types registered by the application.

You can configure the transmission of events to recipient systems (for example, to a SIEM system). Recipient systems that receive application events are called *recipients*. Each recipient has a separate column in the table containing the list of event types. In this column, you can select check boxes to enable transmission of specific event types to a recipient.

The bar with control buttons for the list of event types is located in the lower part of the **Configure events** tab:

- **Add** – adds an event type.

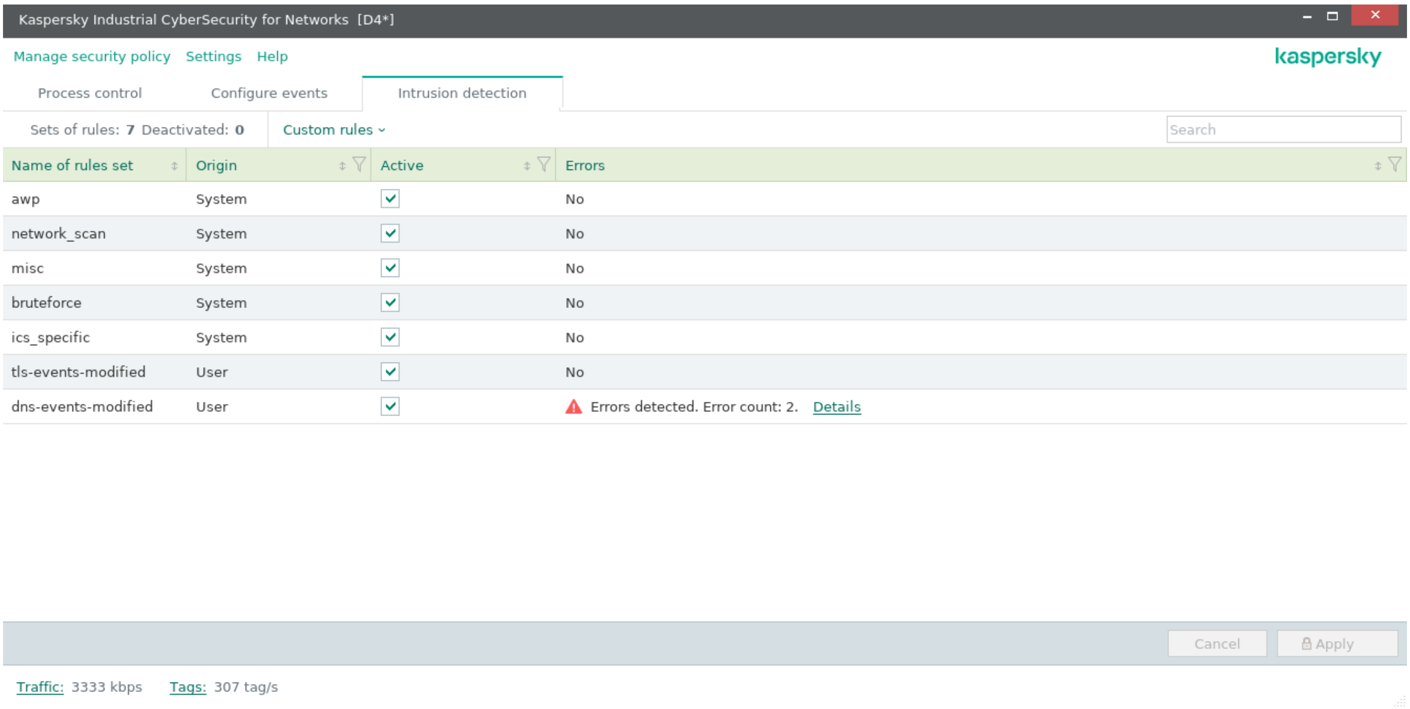
- **Edit** – changes the selected event type.

- **Remove** – removes the selected event type.

- **Specify recipient** – adds a recipient.

Intrusion detection tab

On the **Intrusion detection** tab (see the figure below), you can manage sets of Intrusion Detection rules and additional Intrusion Detection methods.



Sets of rules: 7 Deactivated: 0

Name of rules set	Origin	Active	Errors
awp	System	☑	No
network_scan	System	☑	No
misc	System	☑	No
bruteforce	System	☑	No
ics_specific	System	☑	No
tls-events-modified	User	☑	No
dns-events-modified	User	☑	⚠ Errors detected. Error count: 2. Details

Intrusion detection tab

Above the table containing the sets of Intrusion Detection rules, a toolbar provides the following management elements and data fields:

- **Sets of rules** – total number of rule sets in the table. The sets of rules include Intrusion Detection rules grouped by certain attributes. System sets and custom sets of rules can be used in the application.

- **Deactivated** – number of inactive sets of rules in the table.

- **Custom rules** – menu for selecting actions to take on custom sets of rules. You can use the menu items to load custom sets of rules into the application or remove all custom sets of rules.

- Search field – lets you enter a query to search by values in the **Name of rules set** column.

The table containing the sets of Intrusion Detection rules is located in the main part of the tab. The table columns display the following information about sets of rules:

- **Name of rules set** – name of the set of Intrusion Detection rules. For custom rule sets, the name matches the name of the file from which the rule set was loaded (without the RULES extension).

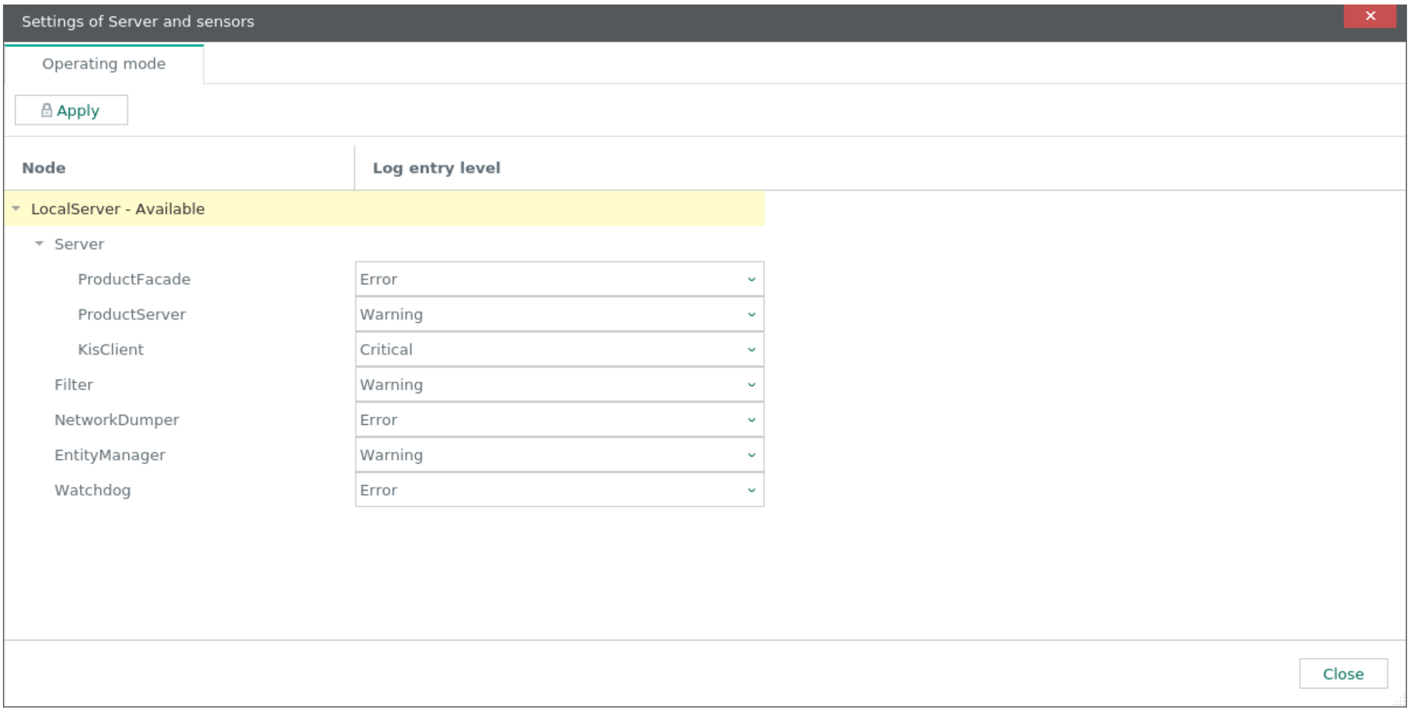
- **Origin** – value determining the type of rule set. Two values are available: **System** (for the system set of rules) or **User** (for the custom set of rules).

- **Active** – field for enabling and disabling rules. If the check box is selected, the rule set is active (rules from the rule set are applied when intrusions are detected). If the check box is cleared, the rule set is inactive (rules from the rule set are not applied). The state of rule sets is modified after the changes are applied.
- **Errors** – information about the presence of errors in rules. If errors have not been detected, the **No** value is displayed. If there are errors, the number of detected errors is displayed. You can open a window containing additional information about errors by clicking the **Details** link (this link appears if there are errors).

The lower part of the **Intrusion detection** tab contains buttons for canceling and applying changes to the state of sets of rules (in the **Active** column).

Settings of Server and sensors window

The **Settings of Server and sensors** window (see the figure below) opens when **Server and sensors** is selected in the **Settings** menu of the Console window.



Node	Log entry level
LocalServer - Available	
Server	
ProductFacade	Error
ProductServer	Warning
KisClient	Critical
Filter	Warning
NetworkDumper	Error
EntityManager	Warning
Watchdog	Error

Settings of Server and sensors window

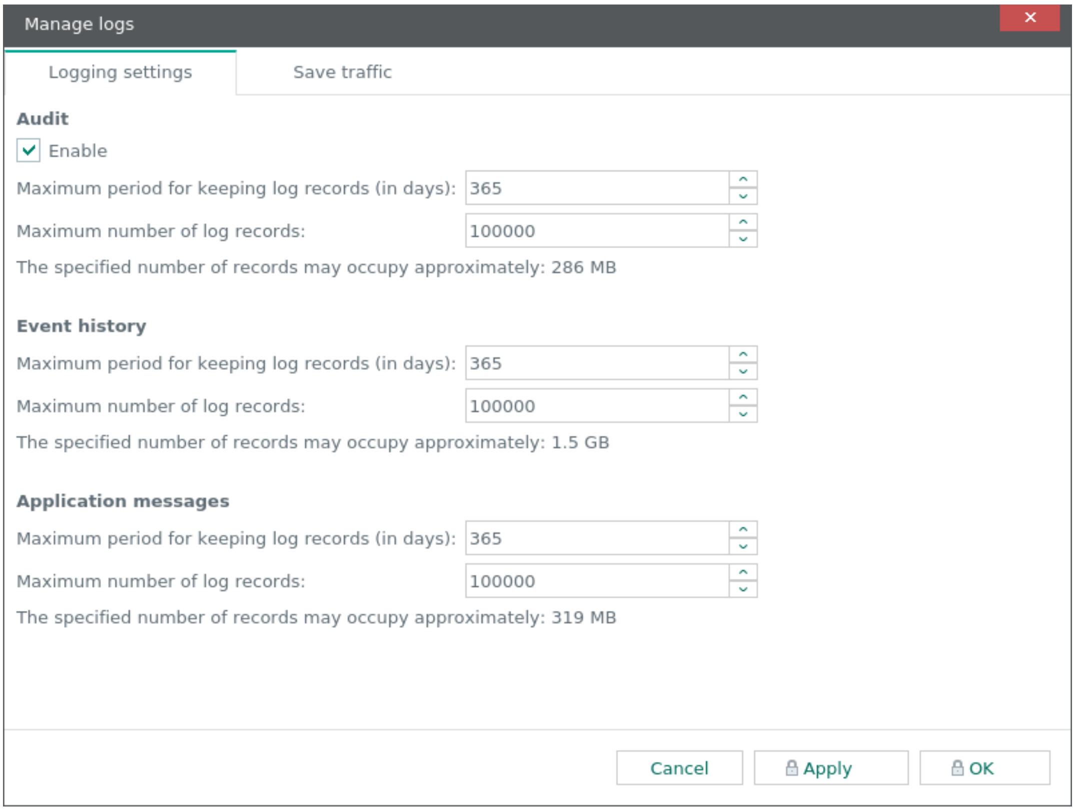
The **Settings of Server and sensors** window contains the **Operating mode** tab. The upper part of the tab contains an **Apply** button that you can use to apply the changes made to process log levels.

Below is a table containing the main information about nodes with Kaspersky Industrial CyberSecurity for Networks Server and sensors installed. The table columns display the following information:

- **Node** – name and current state of the node (*Available*, *Unavailable*, *Malfunction*, *State unknown*). For each node, you see a list of processes that support the operation of application components.
- **Log level** – selected log levels for process logs.

Manage logs window

The **Manage logs** window (see the figure below) opens when **Logs** is selected in the **Settings** menu of the Console window.



Audit

☑ Enable

Maximum period for keeping log records (in days): 365

Maximum number of log records: 100000

The specified number of records may occupy approximately: 286 MB

Event history

Maximum period for keeping log records (in days): 365

Maximum number of log records: 100000

The specified number of records may occupy approximately: 1.5 GB

Application messages

Maximum period for keeping log records (in days): 365

Maximum number of log records: 100000

The specified number of records may occupy approximately: 319 MB

Manage logs window

The **Manage logs** window contains the following tabs:

- **Logging settings** – for changing the settings for storing logs in the database, and for enabling and disabling the user activity audit.
- **Save traffic** – to change the settings for saving traffic in the application database.

Logging settings tab

The **Logging settings** tab contains the **Audit**, **Event history** and **Application messages** settings groups in which you can manage the settings for storing logs in the database. Entries are saved in logs according to the values specified for the following settings:

- **Maximum period for keeping log records (in days)**
- **Maximum number of log records**

You can use the **Enable** check box in the **Audit** settings group to enable and disable the user activity audit.

Save traffic tab

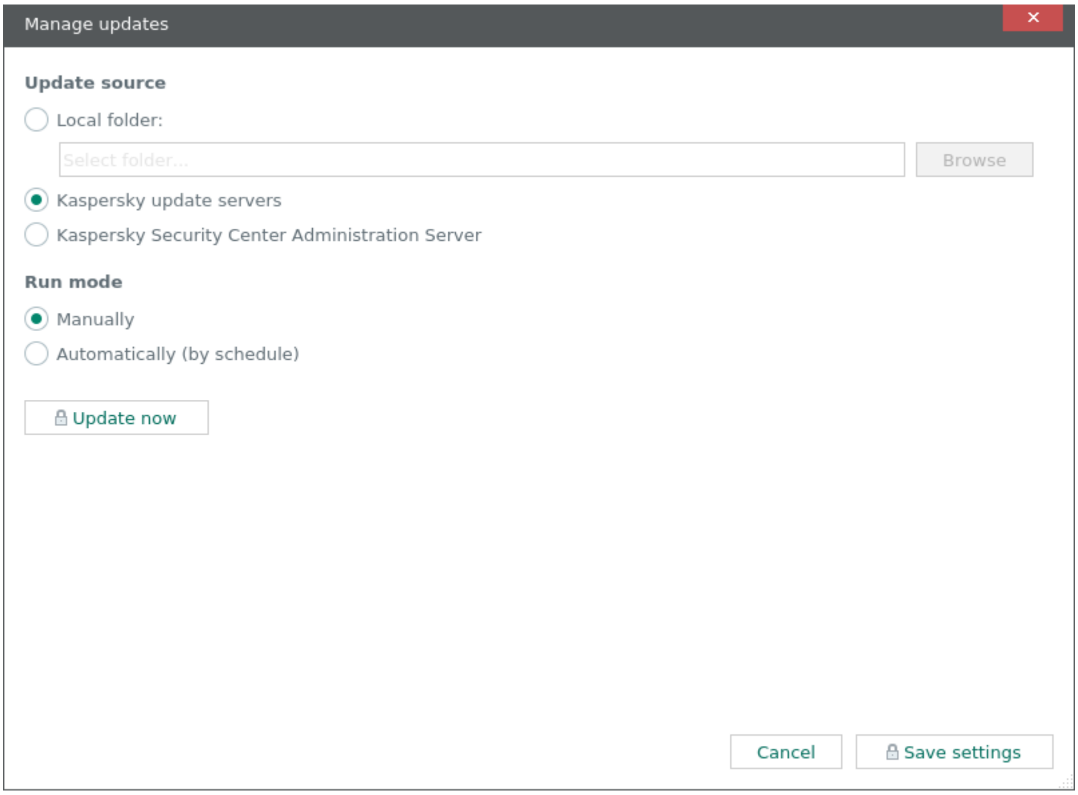
The **Save traffic** tab contains the **Settings for saving traffic** settings group in which you can manage the settings for saving traffic. Traffic data is saved in the database according to the values that are defined by the following settings:

- **Maximum number of saved packets**
- **Maximum period for storing packets (in days)**

- Maximum size of saved traffic in the database (MB)

Manage updates window

The **Manage updates** window (see the figure below) opens when **Update** is selected in the **Settings** menu of the Console window. In this window, you can configure updates of application modules and databases.



Manage updates

Update source

○ Local folder:

Select folder... | Browse

● Kaspersky update servers

○ Kaspersky Security Center Administration Server

Run mode

● Manually

○ Automatically (by schedule)

Manage updates window

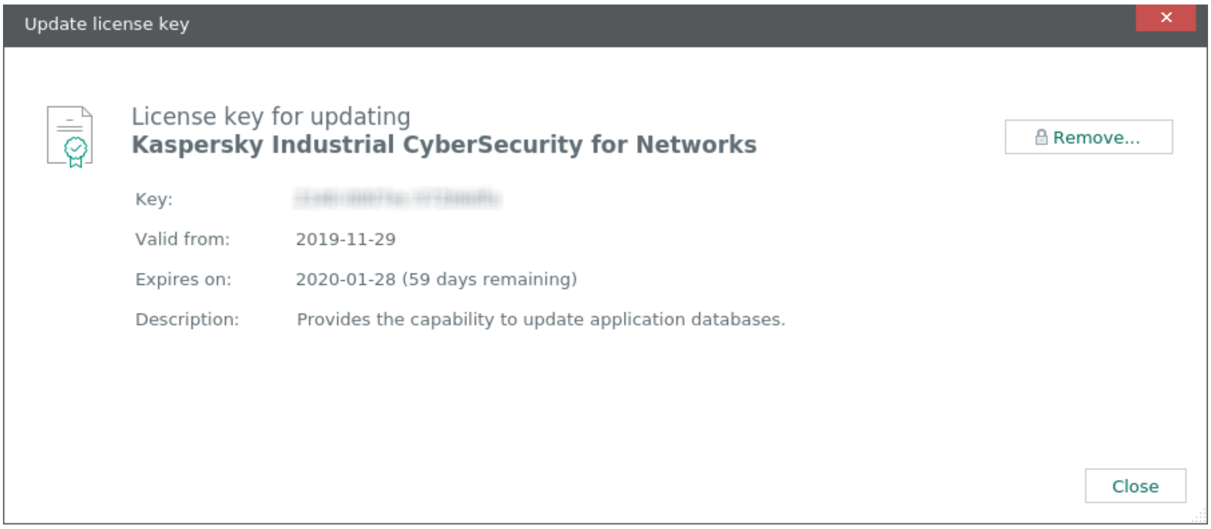
The **Manage updates** window contains the following elements:

- A panel containing a message about the update license key and the **Proceed to add a key** button are displayed if a license key has not been added or if there were problems with the added key. You can use the **Proceed to add a key** button to open the window for adding a license key.
- Management elements for configuring updates (available after a license key is added):
  - **Update source** settings group – for selecting the source of updates for databases and application modules. Your specified update source can be a local folder on a computer that performs Server functions, Kaspersky update servers, or the Kaspersky Security Center Administration Server.
  - **Run mode** settings group – for selecting the update run mode. You can select the **Automatically (by schedule)** option and define a run schedule. You can also select the **Manually** option to disable the run schedule.
  - The **Update now** button is for starting an update right now.

The lower part of the **Manage updates** window has buttons for canceling and saving changes in the settings for updating databases and application modules.

Update license key window

The **Update license key** window (see the figure below) opens when **License key** is selected in the **Help** menu of the Console window. In this window, you can manage the license key for updating application modules and databases.



License key for updating
Kaspersky Industrial CyberSecurity for Networks

Key: [redacted]

Valid from: 2019-11-29

Expires on: 2020-01-28 (59 days remaining)

Description: Provides the capability to update application databases.

Update license key window

Depending on whether or not a license key has been added, the **Update license key** window may contain various information and control elements.

If a license key has not been added to the application, the window contains a warning about the absent key and the **Add key** button.

If a license key has been added, the window contains the following information:

- **Key** – unique alphanumeric sequence.
- **Valid from** – date when the license key was added to the application.
- **Expires on** – date when the license key expires, and the number of days remaining.
- **Description** – information about available functionality.
- Warning about an issue with the license key (if any).

The right part of the window displays the **Remove** button for removing a license key from the application.

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.

> Please 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 the installation of Kaspersky Industrial CyberSecurity for Networks.
- By reading the license_en.txt file. This file is included in the application distribution kit, and is saved in the application installation folder.

Please read and accept the terms of the End User License Agreement during installation of the application. If you do not accept the terms of the End User License Agreement, you must cancel the installation 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.

> Please 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 the installation of Kaspersky Industrial CyberSecurity for Networks.
- By reading the privacy_policy_en.txt file. This file is included in the application distribution kit, and is saved in the application installation folder.

Please read and accept the terms of the Privacy Policy during installation of the application. If you do not accept the terms of the Privacy Policy, you must cancel the installation 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 available:

- Base – for use of all functionality of the Server and sensors, except update functionality for databases and application modules.

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

- Limited Updates – for use of update functionality for databases and application modules on the Server and sensors.

  This type of license has a time limit. To activate update functionality, you need to add a license key to the application. When this type of license expires, the application continues to work, but update functionality becomes unavailable. In this case, to continue to use the application with available update functionality, you need to add a new license key.

  You can view information about the added license key in the Application Console.

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 update functionality

A *license key* (hereinafter also referred to as simply the "key") is a sequence of bits that you can apply to activate and then use the functionality for updating databases and application modules in accordance with the terms of the End User License Agreement. 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 blacklist a license key over violations of the End User License Agreement. If a license key has been blocked, you must add a different license key to use the functionality for updating databases and application modules.

About the license key file used for activating update functionality

A *license key file* is a file with the KEY extension that you receive from Kaspersky. A license key file is intended for adding a license key that activates the functionality for updating databases and application modules.

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 have to connect to Kaspersky activation servers to activate the functionality for updating databases and application modules using a license key file.

Adding a license key in the Application Console

You can add a license key to Kaspersky Industrial CyberSecurity for Networks by using the Application Console or using the functionality for automatic distribution of license keys to Kaspersky Security Center.

When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, you cannot add a license key.

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

To add a license key in the Application Console:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Help** menu in the Console window, select **License key**.

   The screen displays the **Update license key** window.
3. Click the **Add key** button. This button is absent if a license key has already been added to the application.

   The license key file selection window appears on the screen.
4. Specify the path to the folder and the name of 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. Information about the added license key will be displayed in the **Update license key** window.

Viewing information about an added license key in the Application Console

In the Kaspersky Industrial CyberSecurity for Networks Console, you can view information about the added license key. Information about the license key is displayed in the **Update license key** window. A license key status warning may also be displayed in the Console status bar.

When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, you cannot view information about the added license key.

Information about the license key in the status bar

The status bar is displayed on all Console tabs in the lower part of the Console window.

If there are warnings about the license key status, the status bar shows the warning icon and a text description.

The color of the warning icon signifies the importance level (severity) of the problem. The text description of the warning contains more detailed information. If a description is not fully displayed, you can move the cursor over the warning icon to bring up a tooltip with the full description.

The warning icon may have one of the following colors:

- Red

  Update functionality is not available (for example, because the license key expired).

- Yellow

  Update functionality is activated but only 14 days or less remain until the license key expires.

If the status bar displays the warning icon and text description, you can use these elements to proceed to the **Update license key** window.

*To proceed to the **Update license key** window using the displayed elements in the status bar:*

Click the license key status warning icon or the text description in the status bar.

Information about the license key in the Update license key window

You can view detailed information about the license key in the **Update license key** window.

*To open the **Update license key** window:*

In the **Help** menu in the Console window, select **License key**.

For an added license key, the **Update license key** window displays the following information:

- **Key** – unique alphanumeric sequence.
- **Valid from** – date when the license key was first added to the application.
- **Expires on** – date when the license key expires, and the number of days remaining.
- **Description** – information about available functionality.
- Warning about an issue with the license key (if any).

Removing a license key in the Application Console

In the Kaspersky Industrial CyberSecurity for Networks Console, 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 application does not provide the functionality for updating databases and application modules. This functionality will be re-activated the next time you add a license key.

When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, you cannot remove a license key.

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

To delete an added license key:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Help** menu in the Console window, select **License key**.

   The screen displays the **Update license key** window.
3. Click the **Remove** button.

   A window with a confirmation prompt opens.
4. Confirm deletion of the license key.

The license key will be removed from the application.

Processing and storing data in Kaspersky Industrial CyberSecurity for Networks

This section contains information about data provision, utilized logs, and folders for storing data.

About data provision

By accepting the terms of the End User License Agreement and the Privacy Policy, you consent to the automatic processing of personal data for the purposes of supporting the operation of the application. For information about how personal data is obtained, processed, and stored, please read the End User License Agreement and the Privacy Policy.

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 operating system of the Server computer and added to the kics4net group (users that work with the Application Console).
- 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 or names of industrial network devices.
- Device information received by the application during traffic analysis using rules for discovering information about devices and communication protocols.
- IP address or name of the computer with Kaspersky Security Center, and IP addresses or names of computers that are recipient systems' servers for receiving events: Syslog server, SIEM server.
- Email addresses of event notification recipients.
- 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 a copy of industrial network traffic).

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

The application saves the received data in logs.

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

If the application 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 Application Console.
  - Files of working data of the Server and sensors.
  - Application installation settings file.
  - 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:
  - kisc4net
  - kics4net-postgresql
  - kics4net-webserver
  - 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 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 application installation settings file, which may contain personal data. The application does not provide access to the list of users who can work with the Application Console. Therefore, the application does not track the reading of this list. However, the application does track startups of application components (for example, the Console) and other connections to the Server that involve verification of user credentials.

When receiving updates from Kaspersky servers, the application transmits the following data necessary for automatic selection of the relevant updates:

- 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.

About logs

Kaspersky Industrial CyberSecurity for Networks saves data on its operation in logs. Depending on the type of log used to save the data, the application uses a database or saves data in files.

Logs saved in the database

The application saves the contents of the following logs in the 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 the transfer of data from the log of events and incidents to recipient systems.

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 log 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.

Folders for storing application data

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

The Kaspersky Industrial CyberSecurity for Networks Server uses the following folders and subfolders for storing data:

- Main folders of the Server:
  - /opt/kaspersky/kics4net/ – Server installation folder.
  - /var/opt/kaspersky/kics4net/ – folder for storing certificates and operational data of Kaspersky Industrial CyberSecurity for Networks.
  - /var/log/kaspersky/kics4net/ – folder for storing process logs related to the Server.
  - /etc/opt/kaspersky/kics4net/ – folder for storing files containing passwords to external systems.
- DBMS folders:
  - /opt/kaspersky/kics4net-postgresql/ – folder for DBMS installation.
  - /var/opt/kaspersky/kics4net-postgresql/ – folder for storing operational data of the DBMS (DBMS configuration, databases and other data).
  - /var/log/kaspersky/kics4net-postgresql/ – folder for storing DBMS process logs.
  - /etc/opt/kaspersky/kics4net-postgresql/ – folder for storing additional files.
- Folders of the Intrusion Detection system:
  - /opt/kaspersky/kics4net-suricata/ – folder for installation of the Intrusion Detection system.
  - /opt/kaspersky/kics4net/share/ids/ – folder for storing operational data of the Intrusion Detection system (Intrusion Detection system configuration, rules and other data).
  - /var/log/kaspersky/kics4net-suricata/ – folder for storing process logs related to the Intrusion Detection system.
- Web server folders:
  - /opt/kaspersky/kics4net-webserver/ – folder for web server installation.
  - /var/opt/kaspersky/kics4net-webserver/ – folder for storing operational data of the web server (files of certificates and other data).
  - /var/log/kaspersky/kics4net-webserver/ – folder for storing process logs of the Web Server (the Web Server also saves process data in the system log of the operating system).
- Folders containing files for installing application components:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were installed from this computer).
  - /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file.
- Folders of the application Console:
  - /opt/kaspersky/kics4net/ – Console installation folder.
  - /home/<user>/.config/kaspersky/kics4net/ – folder for storing operational data of the Console (configuration file and other data).

- Network Agent folders:
  - /opt/kaspersky/klnagent64/ – Network Agent installation folder.
  - /var/opt/kaspersky/klnagent/ – folder for storing operational data of Network Agent.
  - /var/log/kaspersky/klnagent64/ – folder for storing process logs of Network Agent.
  - /etc/opt/kaspersky/klnagent/ – folder for storing Network Agent configuration files.
- Standard folders of the operating system:
  - /usr/lib/systemd/system/ – folder for storing configuration files for services (for example, kics4net.service).
  - /var/run/ – folder for storing variables of data on system health after loading. Application components may store files in the folder itself (for example, the file klnagent.pid) or in subfolders (for example, in the subfolder /kics4net/).

A Kaspersky Industrial CyberSecurity for Networks sensor uses the following folders and subfolders for storing data:

- Main folders of a sensor:
  - /opt/kaspersky/kics4net/ – sensor installation folder.
  - /var/opt/kaspersky/kics4net/ – folder for storing certificates and operational data of Kaspersky Industrial CyberSecurity for Networks.
  - /var/log/kaspersky/kics4net/ – folder for storing process logs related to a sensor.
- Folders of the Intrusion Detection system:
  - /opt/kaspersky/kics4net-suricata/ – folder for installation of the Intrusion Detection system.
  - /opt/kaspersky/kics4net/share/ids/ – folder for storing operational data of the Intrusion Detection system (Intrusion Detection system configuration, rules and other data).
  - /var/log/kaspersky/kics4net-suricata/ – folder for storing process logs related to the Intrusion Detection system.
- Folders containing files for installing application components:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were installed from this computer).
  - /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file.
- Standard folders of the operating system:
  - /usr/lib/systemd/system/ – folder for storing configuration files for services (for example, kics4net.service).
  - /var/run/ – folder for storing variables of data on system health after loading. Application components may place files in the folder itself or in subfolders.

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

Administration of Kaspersky Industrial CyberSecurity for Networks

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

Managing monitoring points

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.

You can manage monitoring points and view information about monitoring points, network interfaces and nodes on the **Deployment** tab in the **Settings** section of the web interface of Kaspersky Industrial CyberSecurity for Networks.

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 a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section.
3. On the **Deployment** tab, 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 Latin alphabet, numerals, and the _ and - characters.

   The monitoring point name must meet the following requirements:

   - Must be unique (not assigned to another monitoring point).
   - Contains from 1 to 100 characters.
5. Click the ✓ icon on the right of the entry field.

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 a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section.
3. On the **Deployment** tab, perform one of the following actions:

   - If you want to enable one monitoring point, click the **Enable** button in the tile of the network interface 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 tile of the node 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 a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section.

3. On the **Deployment** tab, perform one of the following actions:

   - If you want to disable one monitoring point, click the **Disable** button in the tile of the network interface 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 tile of the node 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 a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section.

3. On the **Deployment** tab, select the tile of the network interface 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 ✎ icon located on the right of the current name of the monitoring point, and enter the new name in the field that appears.

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

   The monitoring point name must meet the following requirements:

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

5. Click the ✓ icon on the right of the entry field.

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 delete a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section.
3. On the **Deployment** tab, select the tile of the network interface 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 a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section.

3. On the **Deployment** tab, 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.

Monitoring the state of Kaspersky Industrial CyberSecurity for Networks

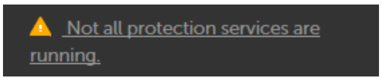
This section contains instructions on monitoring the state of the application.

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 a web browser.

Information about disabled protection functions

In the web browser window, the lower part of the menu shows the ⚠ icon and a notification if some protection functions are disabled (see the figure below).



⚠ Not all protection services are running.

Message about disabled protection functions in the web browser window

The ⚠ icon 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).

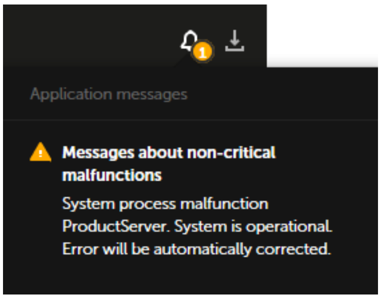
- Learning mode is enabled for one or multiple protection functions (for example, for Network Integrity Control technology).

To view information about disabled protection functions:

Click the ⚠ icon or the text of the message about disabled 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).



⚠ **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 web 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 web browser window shows a section containing information pertaining to the notification (for example, the **Application messages** tab in the **Settings** section).

Information about the current state of the application

You can view information about the current state of the application in the Tags section. The **Application state** field displays the status as the presence or absence of problems in application operation.

If the application is running normally, the **Application state** field displays the *No problems detected* status.

If the *An error occurred* or *Unknown* status is displayed, industrial network protection functions may be only partially operational. You need to take steps to restore normal operation of the application.

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.

To view application messages:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser.
2. Select the **Settings** section and go to the **Application messages** tab.

   The table will display application messages that match the defined filter and search settings.

The columns of the application messages table contain the following information:

- **Date and time** – date and time of registration of the application message.
- **Status** – name of the message status. The following statuses are available for messages:
  - *Getting started*, *Normal operation* – for informational messages.
  - *State 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 following functions:

- Filtering based on standard periods

  When filtering based on a standard period, the application messages table is updated in online mode.

  To configure application message filtering based on a standard period:

  1. On the **Application messages** tab, in the **Settings** section, perform one of the following actions:
     - Open the **Period** drop-down list in the toolbar.
     - Click the filtering icon in the **Date and time** column.
  2. In the drop-down list, select one of the standard periods:
     - Last hour
     - Last 12 hours
     - Last 24 hours
     - Last 48 hours
  3. If table updates are disabled, in the opened window confirm that you agree to resume table updates.

     The table will display application messages for the period you specified.

- Filtering based on a specified period

When filtering by a defined period, the table will no longer be updated. The table displays only the messages that were registered during the specified period.

To configure application message filtering based on a specified period:

1. On the **Application messages** tab, in the **Settings** section, perform one of the following actions:
   - Open the **Period** drop-down list in the toolbar.
   - Click the filtering icon in the **Date and time** column.
2. In the drop-down list, select **Specify a period**.
3. If table updates are enabled, in the opened window confirm that you agree to suspend table updates.

   On the right of the **Period** drop-down list in the toolbar, you will see additional buttons that you can use to manually define the filtering period.
4. Click any of the buttons containing a date and time value in the **From** and **to** fields.

   The calendar opens.
5. In the field under the calendar on the left, specify the date and time for the start boundary of the filtering period. In the field under the calendar on the right, specify the date and time for the end boundary of the filtering period. If you want to remove the limit for the end boundary of the period, delete the value in the field under the calendar on the right.

   To enter a value in the field, you can select a date in the calendar (the current time will be indicated) or manually enter the necessary value in the format DD-MM-YYYY hh:mm:ss.
6. Click **OK**.

The table will display application messages for the period you specified.

- Filtering based on table columns ?

When filtering by the **Date and time** column, you can use one of the standard periods or define a specific period.

*To filter the application messages table by the **Status** or **System process** column:*

1. On the **Application messages** tab in the **Settings** section, click the filtering icon in the relevant column.

   When filtering by status, you can also use the **Statuses** drop-down list in the toolbar.

   The filtering window opens.
2. Select the check boxes opposite the values by which you want to filter events.
3. Click **OK**.

*To filter the application messages table by the **Node** or **Message** column:*

1. On the **Application messages** tab in the **Settings** section, click the filtering icon in the relevant column.

   The filtering window opens.
2. In the **Including** and **Excluding** fields, enter the values for application messages that you want to include into the filter and/or exclude from the filter.
3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window of the column click the **Add condition** button and enter the condition in the opened field.
4. If you want to delete one of the created filter conditions, in the filter window of the column click the 🗑 icon.
5. Click **OK**.

- Searching application messages ?

To find relevant application messages:

On the **Application messages** tab, in the **Settings** section, enter your search query into the **Search messages** field. The search is initiated as you enter characters.

The application messages table displays entries that meet the search criteria.

The search is performed based on the **Node** and **Message** columns.

- Resetting the defined filter and search settings ?

To reset the defined filter and search settings in the application messages table:

On the **Application messages** tab in the **Settings** section, click the **Clear filter** button in the toolbar (this button is displayed if the filter and/or search settings are defined).

- Sorting application messages

To sort application messages:

1. On the **Application messages** tab in the **Settings** section, click the header of the column by which you want to sort.
2. 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.

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.

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 a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Audit** tab.

   The table will display the audit entries that match the defined filter and search settings.

The columns of the audit entries table contain the following information:

- **Date and time** – date and time when the user activity 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.
- **Node** – IP address of the node on which the registered action was performed.
- **Description** – additional information about the registered action.

When viewing the audit entries table, you can use the following functions:

- Configure the display and order of columns in the audit entries table

To configure the list of columns displayed in the table:

1. On the **Audit** tab in the **Settings** section, click the **Customize table** button.

   A window opens for configuring the display of the audit entries table.

2. Select the check boxes opposite the settings that you want to view in the table. You must select at least one setting.

3. 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 audit entries table in the order you specified.

- Filtering based on standard periods

When filtering based on a standard period, the audit entries table is updated in online mode.

To configure filtering of audit entries based on a standard period:

1. On the **Audit** tab in the **Settings** section, perform one of the following actions:

   - Open the **Period** drop-down list in the toolbar.

   - Click the filtering icon in the **Date and time** column.

2. In the drop-down list, select one of the standard periods:

   - **Last hour**

   - **Last 12 hours**

   - **Last 24 hours**

   - **Last 48 hours**

3. If table updates are disabled, in the opened window confirm that you agree to resume table updates.

The table will display audit entries for the period you specified.

- Filtering based on a specified period

When filtering by a defined period, the table will no longer be updated. The table displays only the entries that were registered during the specified period.

To configure filtering of audit entries based on a specified period:

1. On the **Audit** tab in the **Settings** section, perform one of the following actions:

   - Open the **Period** drop-down list in the toolbar.

   - Click the filtering icon in the **Date and time** column.

2. In the drop-down list, select **Specify a period**.

3. If table updates are enabled, in the opened window confirm that you agree to suspend table updates.

   On the right of the **Period** drop-down list in the toolbar, you will see additional buttons that you can use to manually define the filtering period.

4. Click any of the buttons containing a date and time value in the **From** and **to** fields.

   The calendar opens.

5. In the field under the calendar on the left, specify the date and time for the start boundary of the filtering period. In the field under the calendar on the right, specify the date and time for the end boundary of the filtering period. If you want to remove the limit for the end boundary of the period, delete the value in the field under the calendar on the right.

   To enter a value in the field, you can select a date in the calendar (the current time will be indicated) or manually enter the necessary value in the format DD-MM-YYYY hh:mm:ss.

6. Click **OK**.

The table will display audit entries for the period you specified.

- Filtering based on table columns

You can filter the audit entries table based on the values in all columns except the **Description** column.

When filtering by the **Date and time** column, you can use one of the standard periods or define a specific period.

*To filter the audit entries table by the **Action** or **Result** column:*

1. On the **Audit** tab, in the **Settings** section, click the filtering icon in the relevant column.
   When filtering by the results of actions, you can also use the corresponding buttons in the toolbar.
   The filtering window opens.
2. Select the check boxes opposite the values by which you want to filter events.
3. Click **OK**.

*To filter the audit entries table by the **User** or **Node** column:*

1. On the **Audit** tab, in the **Settings** section, click the filtering icon in the relevant column.
   The filtering window opens.
2. In the **Including** and **Excluding** fields, enter the values for audit entries that you want to include into the filter and/or exclude from the filter.
3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window of the column click the **Add condition** button and enter the condition in the opened field.
4. If you want to delete one of the created filter conditions, in the filter window of the column click the 🗑 icon.
5. Click **OK**.

- Searching for audit entries ?

To find relevant audit entries:

On the **Audit** tab, in the **Settings** section, enter your search query into the **Search records** field. The search is initiated as you enter characters.

The audit entries table will display the entries that meet the search criteria.

A search is performed in all columns except the **Date and time** and **Result** columns.

- Resetting the defined filter and search settings ?

To reset the defined filter and search settings in the audit entries table:

On the **Audit** tab in the **Settings** section, click the **Clear filter** button in the toolbar (this button is displayed if search or filter settings are defined).

- Sorting audit entries ?

To sort audit entries:

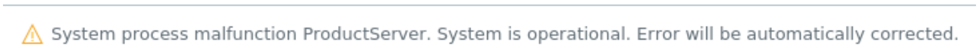
1. On the **Audit** tab in the **Settings** section, click the header of the column by which you want to sort.
   You can filter the audit entries table based on the values of any column except the **Description** column.
2. If you need to sort the table based on multiple columns, press the `SHIFT` key 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.

Monitoring the application state in the Kaspersky Industrial CyberSecurity for Networks Console

In the Kaspersky Industrial CyberSecurity for Networks Console, you can view information about the current state of the application in the status bar. The status bar is displayed in the lower part of the Console window.

If there are problems in the application, a notification icon and text description of the problem will be displayed in the status bar (see the figure below).



⚠ System process malfunction ProductServer. System is operational. Error will be automatically corrected.

Application state

The color of the notification icon signifies the severity of the problem. The text description contains more detailed information about the problem. If a description is not fully displayed, you can move the cursor over the problem's notification icon to bring up a tooltip with the full description.

The problem's notification icon may have one of the following colors:

- Red

  There is no connection between the Server and the Console, or the connection is established but the following problems have been detected:

  - One of the application processes has crashed on the Server.

  - The application has no access to the database.

- Yellow

  Problems that are not critical for the application have been detected on one or more nodes (application processes continue running).

- Gray

  The application state is unknown; information about the state of the application is being refreshed.

If the application is not experiencing any problems, a problem notification icon is not displayed in the status bar.

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 a web browser.

2. Select the **Settings** section.

   The **Deployment** tab displays tiles of nodes (on the left) and tiles of the network interfaces detected on these nodes (on the right of each node).

3. If you want to view expanded information (including displaying the names of fields), 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

The following information is displayed for nodes:

- Node name defined during installation of application components on this node.

- Current state of the node indicated as an icon and text description (in the details area, the icon and text description are displayed in the **State** field). Possible states:

  - ⓘ *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 *State unknown* or *Malfunction* status were received from this node.

  - ❗ *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.

- IP address (it is displayed in the **IP address** field in the details area).

- Application component installed on the node: **Server** or **Sensor** (it is displayed in the **Node type** field in the details area).

Displayed information about network interfaces

The following information is displayed for network interfaces:

- Icon showing if a network cable is connected to the Ethernet port of the network interface (it is displayed in the **Connection** field in the details area). The following icons are provided:

  - ● – the network cable is connected.

  - ○ – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.

- Name of the network interface in the operating system (it is displayed in the **Network interface** field in the details area).

- MAC address (it is displayed in the **MAC address** field in the details area).

- IP address. If multiple IP addresses are detected on a network interface, the network interface tile displays only one of them and the details area displays no more than 16 IP addresses.

- Rate of incoming traffic received by the network interface.

If a monitoring point has been added to the network interface, the following additional information is displayed.

- Monitoring point name.

- Current state of the monitoring point indicated as an icon and text description (in the details area, the icon and text description are displayed in the **State** field). Possible states:

  - ⓘ *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.

- Current operating mode of the monitoring point. In the network interface tile, information about the current mode is displayed next to the current status field (except the *Switchover* state. In the details area, information about the current state is displayed in the **Mode** field. The following modes are provided:

    - *Enabled*.

    - *Disabled*.

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 on a computer that performs Server functions or sensor functions)

    - `kics4net-postgresql` – DBMS service (runs only on a computer that performs Server functions)

    - `kics4net-webserver` – Web Server 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 the 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 restart
     sudo service kics4net-webserver restart
     ```
   - If the computer performs sensor functions, enter the following command:
     ```
     sudo service kics4net 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 Network 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 assets in the assets table. Use of asset 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.

Synchronizing Server time with the time source for industrial network assets

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 assets.

When installing Kaspersky Industrial CyberSecurity for Networks, you can enable time synchronization between the Server and nodes on which sensors are installed. In this case, the node with the Server installed will serve as the time source for nodes that have sensors installed.

The Network Time Protocol (NTP) is used for automatic configuration of time synchronization between the Server and other nodes. In this case, you cannot configure synchronization with other time sources or use the Precision Time Protocol (PTP) on 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 application Server and the time source used by assets in the industrial network. You can use the standard NTP and PTP protocols to synchronize the Server time. You can find an example of how to configure time synchronization in the Knowledge Base on the Kaspersky website.

Updating SSL connection certificates

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

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 to Kaspersky Industrial CyberSecurity for Networks through the API.

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:

1. On the computer from which the installation was performed, go to the folder containing the saved files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks.
2. Enter the command for running the application installation script with the `update-certs` parameter:
   ```
   bash kics4net-deploy-<application version number>.bundle.sh --update-certs
   ```
3. In the `SSH password` and `SUDO password` invitations, enter the password for the user account that is used to run the installation.

   Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh. Upon successful completion, a success notification will appear on the screen.

The application will begin to use the updated certificates on all nodes that have installed components of Kaspersky Industrial CyberSecurity for Networks.

Updating certificates for connecting to Kaspersky Industrial CyberSecurity for Networks through the web interface

You can update certificates used for connecting to the Server through the web interface when reinstalling Kaspersky Industrial CyberSecurity for Networks. To update certificates, in the main installation menu select **Change Server settings** → **Change Web Server certificate settings** and choose one of the following certificate options:

- If you want to update self-signed certificates, enter `y` at the **Use self-signed certificates to connect to web server** prompt.
- If you want to update trusted certificates, enter `y` at the **Use trusted certificates to connect to web server** prompt and then enter the path to the file of the trusted certificate.

Certificates will be updated after reinstallation of Kaspersky Industrial CyberSecurity for Networks.

Updating certificates for connecting to Kaspersky Industrial CyberSecurity for Networks through the API

You can update certificates used for connecting to Kaspersky Industrial CyberSecurity for Networks through the API when reinstalling Kaspersky Industrial CyberSecurity for Networks. To update certificates, in the main installation menu select **Change Server settings** → **Change the settings for connecting to the Server via API** and type `y` at the **Generate new certificates** prompt.

Certificates will be updated after reinstallation of Kaspersky Industrial CyberSecurity for Networks.

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.
- Rules for obtaining information about devices and communication protocols.
- Event correlation rules for registering incidents.
- Modules for processing application-layer protocols for Deep Packet Inspection.

Timely updates of databases and application modules ensure maximum protection of the industrial network using Kaspersky Industrial CyberSecurity for Networks. It is recommended to update databases and application modules immediately after installing components of Kaspersky Industrial CyberSecurity for Networks, and then configure the settings for automatic installation of updates.

You can use the following update sources:

- Kaspersky update servers.
- Local folder on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server.
- Kaspersky Security Center Administration Server.

Installation of updates may be started automatically according to a defined schedule, or manually.

You can use the Kaspersky Industrial CyberSecurity for Networks Console to manually configure the settings for installing updates. You can view information about installed updates in the Application Console (only general information) or when connected to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser (general information, and additional information saved in application messages).

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.
- 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 a local folder, the kics4net group must be granted access to this folder. Use the standard tools of the operating system to grant access to the folder.
- There is no support for downloading updates from folders on other computers over remote access protocols (FTP, NFS, SMB, and others). To download updates over a remote access protocol, you can connect a network resource (folder containing updates to be downloaded) on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server. The network resource can be connected using the standard tools for mounting network resources in the operating system. After connecting the network resource, you can select a local folder to be mounted as the source of updates.

- To download updates from the Kaspersky Industrial CyberSecurity for Networks Administration Server to Kaspersky Industrial CyberSecurity for Networks, the capability for application interaction with Kaspersky Security Center must be added. You can specify the settings for relaying events and application state to Kaspersky Security Center when installing or reinstalling 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.

Selecting an update source

After adding a license key, you can select one of the following sources of updates for databases and application modules:

- Kaspersky update servers.
- Local folder on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server.
- Kaspersky Security Center Administration Server.

Only users with the Administrator role can select an update source.

To select an update source:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Update**.

   The **Manage updates** window opens.
3. In the **Update source** settings group, select one of the following options for update sources:
   - **Local folder** – for downloading updates from a specified local folder on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server.
   - **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. If the **Local folder** option is selected, specify the path to the folder in the local file system. You can use the **Browse** button to open the window for selecting a folder.

   > The kics4net group must be granted access to the specified folder. If necessary, grant access to this folder using the standard tools of the operating system.
5. Click the **Save settings** button.

Selecting the update run mode

After adding a license key, you can select one of the following modes for starting updates of databases and application modules:

- Manually.
- Automatically according to a defined schedule.

Only users with the Administrator role can select the update run mode.

To select the update run mode:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Update**.

   The **Manage updates** window opens.
3. In the **Run mode** settings group, select one of the following options for starting an update:
   - **Manually** – to start an update only manually.
   - **Automatically (by schedule)** – to start an update either according to a schedule or manually.
4. If the **Automatically (by schedule)** option is selected, specify the update schedule settings. To do so:

   a. In the 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.
5. Click the **Save settings** button.

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. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Update**.

   The **Manage updates** window opens.
3. Click the **Update now** 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. This information is displayed in the Application Console or when connected to the Server through a web browser.

To view general information about installed updates in the Application Console:

In the **Help** menu of the Application Console window, select the **About** option.

To view general information about installed updates when connected to the Server through a web browser:

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.

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.

User accounts created in the application are used for restricting user access. Users must use these user accounts to connect to the Server and work with the application. It is not possible to connect under other user accounts or using anonymous connections.

User accounts created in the application do not have to be registered as operating system user accounts on the Server's computer or another computer.

The first application user account must be created during installation of Kaspersky Industrial CyberSecurity for Networks. After installation, you can add application user accounts when connected to the Server through the web interface or when reinstalling the application.

Depending on the method used to connect to the Server, users can access the following sets of functions:

- Application functions available through the web interface
- Application functions available in the Console

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 application user accounts.

- Operator.

  A user with the Operator role has access privileges only for monitoring and viewing information.

The Administrator role is assigned to the user account that is created during installation or reinstallation of Kaspersky Industrial CyberSecurity for Networks. If the name of an already existing user account is specified when reinstalling the application, the role of this user is not changed.

After the application is installed, you can connect to the Server through the web interface under a user account with the Administrator role and generate a list of application user accounts with their corresponding roles. You can create up to 100 application user accounts in the application.

When connected to the Server, users receive the access privileges corresponding to the role of their user account. If the role of a 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 application user accounts on the **Users** tab in the **Settings** section of the Kaspersky Industrial CyberSecurity for Networks web interface.

Application functions available through the web interface

This section 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 when connected through the web interface, 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	✓	✓
Adding a monitoring point	✓	

Enabling monitoring points	✓	
Disabling monitoring points	✓	
Renaming a monitoring point	✓	
Deleting a monitoring point	✓	
Identifying the Ethernet port associated with a network interface	✓	
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 the password of your own user account for connecting through the web interface	✓	✓
Viewing the assets table	✓	✓
Viewing asset information	✓	✓
Creating an asset group tree	✓	
Manually adding assets	✓	
Merging assets	✓	
Deleting assets	✓	
Changing the statuses of assets	✓	
Managing the arrangement of assets in the group tree	✓	
Adding and removing labels for assets	✓	
Editing asset information	✓	
Adding, editing and deleting custom fields for an asset	✓	
Viewing events associated with assets	✓	✓
Viewing the table of Network Control rules	✓	✓
Manually creating Network Control rules	✓	
Editing Network Control rule settings	✓	
Changing the state of a Network Control rule	✓	
Deleting Network Control rules	✓	
Managing technologies	✓	
System monitoring in online mode	✓	✓
Working with the network map	✓	✓
Moving nodes and groups to other groups on the network map	✓	
Monitoring events and incidents	✓	✓
Monitoring process parameters	✓	✓

Application functions available in the Console

This section presents the application functions that are available to users in the Kaspersky Industrial CyberSecurity for Networks Console (see the table below).

Available application functions in the Console, depending on the user role

Application function	Administrator	Operator
Monitoring the application state in the Kaspersky Industrial CyberSecurity for Networks Console	✓	✓
Viewing information about an added license key	✓	✓
Adding a license key	✓	
Removing a license key	✓	
Viewing information about update installation	✓	✓
Selecting an update source	✓	
Selecting the update run mode	✓	
Manually starting an update	✓	
Creating a new security policy	✓	✓
Saving a security policy to a folder	✓	✓
Opening a security policy from a folder	✓	✓
Applying a security policy on the Server	✓	
Loading the current security policy from the Server	✓	✓
Viewing security policy properties	✓	✓
Changing the name of a security policy	✓	✓
Configuring Process Control	✓	✓ (prior to applying a security policy on the Server)
Configuring events	✓	✓ (prior to applying a security policy on the Server)
Viewing the table containing sets of Intrusion Detection rules	✓	✓
Changing the state of sets of Intrusion Detection rules	✓	
Loading and replacing custom sets of Intrusion Detection rules	✓	
Removing custom sets of Intrusion Detection rules	✓	
Managing the settings for storing log entries in the database	✓	
Managing the settings for saving traffic in the database	✓	
Enabling and disabling the user activity audit	✓	
Changing the log level for processes	✓	

Viewing information about application user accounts

Only users with the Administrator role can view information about application user accounts.

To view information about application user accounts:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section and go to the **Users** tab.

   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 a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section and go to the **Users** tab.

3. On the **Users** tab, 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 Latin alphabet, numerals, a dot, 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.

   You can use uppercase and lowercase letters of the Latin alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`.

   The password must meet the following requirements:

   - Must contain from 8 to 20 characters.
   - Must contain one or more uppercase letters.

- Must contain one or more lowercase letters.
- Must contain one or more numerals.

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

Only users with the Administrator role can change the role of an application user account.

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 a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Users** tab.
3. On the **Users** tab, 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

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 a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Users** tab.
3. On the **Users** tab, click the **Delete** button in the tile of the user 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 the Kaspersky Industrial CyberSecurity for Networks web interface opens, you can change the password of your user account that was used to connect to the Server.

You are advised to change the password in the following cases:

- You are connecting for the first time after the user account was created.
- 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 user account:

1. In the web browser window 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 **Password change** 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 **Password change** 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 for the next connection to the Server through a web browser or through the Application Console.

Security policies

A *security policy* is a set of data that defines the following operational settings of the application:

- Process Control settings
- Registration settings for event types

The other application operation settings (including the settings of Asset Management, Network Control, and Intrusion Detection) are applied irrespective of the active security policy.

The application registers events and displays process parameter values according to the active security policy currently running on the Server. Only one security policy can be running on the Server at a time.

You can create, edit or open a security policy in the Console. For the Application Server to start operating based on a security policy, the security policy must be applied on the Server. You can create multiple security policies and save them to folders on the computer on which the Application Console is running.

The folder used to store a security policy contains the following set of files for the security policy:

- common
- gate
- industrial
- meta_data
- nic
- ui
- version

> Editing security policy files in any editor other than the Kaspersky Industrial CyberSecurity for Networks Console may lead to a disruption in the operation of Kaspersky Industrial CyberSecurity for Networks if the security policy is applied on the Server. The application may stop performing protection functions for the industrial network.

You can open from a folder on the computer and view a previously saved security policy in the Kaspersky Industrial CyberSecurity for Networks Console. When a security policy is opened, the current security policy is no longer displayed in the Console but continues to run on the Server until a new policy is applied.

In the current version of Kaspersky Industrial CyberSecurity for Networks Console, you cannot open security policies created in a previous version of the application. You can import security policies from the previous version of the application by using the security policy conversion utility.

A security policy can be opened from a folder regardless of the state of the Console's connection to the Kaspersky Industrial CyberSecurity for Networks Server. If there is no connection to the Server, the **Process Control** and **Configure events** tabs in the Application Console display the data of the opened policy. In addition, the window of the Application Console displays a notification stating that there is no connection to the Server.

If you want to view the active security policy in the Console, you can load the current security policy from the Server. The Console needs to be connected to the Server to load the security policy from the Server.

In the **Security policy properties** window, you can view general information about the security policy open in the Console and about the security policy running on the Server. This window displays the following information:

- **Name** – name of the security policy.
- **Applied** – time last applied on the Server (for a security policy that is running on the Server).
- **Saved** – time last saved to a folder (for a security policy that is open in the application Console).
- **ID** – identifier of the security policy instance.

- **Path** – path to the folder in which the security policy was saved (for a security policy that is open in the application Console).

Creating a new security policy

You can create a new security policy when working with the Application Console.

The settings defined in the created security policy go into effect in Kaspersky Industrial CyberSecurity for Networks after it is applied on the Server.

To create a new security policy:

1. In the **Manage security policy** menu in the Application Console window, select **Create**.
2. If there are unsaved changes in the current security policy, a window opens with a prompt to continue. Perform the necessary action:
   - If you want to save the changes to the current security policy, click **Yes**.
   - If you do not want to save the changes, click **No**.

   A window opens for entering the name of the new security policy.
3. Enter the name of the new security policy and click **OK**. It is recommended to use characters from the Latin alphabet.
4. Configure the Process Control settings and the registration settings for event types.
5. Save the security policy.

Saving a security policy to a folder

The security policy open in the Application Console can be saved as a set of files in a folder.

To save the changes made to the current security policy:

1. In the Console window, open the **Manage security policy** menu.
2. Select **Save**.

To save the security policy with the option of changing its folder:

1. In the Console window, open the **Manage security policy** menu.
2. Select **Save as**.
3. In the window that opens, specify the path to the destination folder for saving the security policy.
4. Click the **Select** button.

Opening a security policy from a folder

You can open a security policy in the following ways:

- Select the folder containing the saved files of the security policy.
- Select a recently opened security policy.

To open a security policy with the option of selecting its folder:

1. In the **Manage security policy** menu in the Console window, select the **Open** option.
2. If there are unsaved changes in the current security policy, a window opens with a prompt to continue. Perform the necessary action:

   - If you want to save the changes to the current security policy, click **Yes**.
   - If you do not want to save the changes, click **No**.

   A window opens for selecting the folder containing the security policy files.
3. Select the folder storing the security policy files.

Data of the open security policy is loaded to the Kaspersky Industrial CyberSecurity for Networks Console. The title of the Console window displays the name of the open security policy.

To open a recently opened security policy:

1. In the **Manage security policy** → **Recent** menu, in the Console window select the name of the security policy that you want to open.
2. If there are unsaved changes in the current security policy, a window opens with a prompt to continue. Perform the necessary action:

   - If you want to save the changes to the current security policy, click **Yes**.
   - If you do not want to save the changes, click **No**.

Data of the selected security policy is loaded to the Kaspersky Industrial CyberSecurity for Networks Console. The title of the Console window displays the name of the selected security policy.

Applying a security policy on the Server

Only users with the Administrator role can apply the current security policy on the Kaspersky Industrial CyberSecurity for Networks Server.

To apply the security policy on the Server:

1. Make sure that the security policy that you want to apply on the Server is displayed in the Application Console.

2. In the **Manage security policy** menu in the window of the Application Console, select the **Apply** option.

3. If the credentials of a user with the Operator role are indicated for the current Console session, a user change prompt window opens. Click **Yes** in the prompt window and enter the name and password of a user with the Administrator role in the next window.

   A window opens with a confirmation prompt to apply the security policy.

4. Confirm the changes made to the security policy. To do so, click **Yes** in the prompt window.

   The screen shows a progress bar showing the process of applying the security policy.

The Server and sensors linked with it automatically begin running according to the new security policy. In the **Security policy properties** window, you can see which security policy is running on the application Server.

Loading a security policy from the Server to the Console

When a security policy is loaded from the Kaspersky Industrial CyberSecurity for Networks Server, the Application Console stops displaying previously opened security policy.

To load the security policy from the Server:

1. In the **Manage security policy** menu in the Console window, select **Load from Server**.

2. If there are unsaved changes in the current security policy, a window opens with a prompt to continue. Perform the necessary action:

   - If you want to save the changes to the current security policy, click **Yes**.

   - If you do not want to save the changes, click **No**.

Data of the security policy applied on the Server is displayed in the Kaspersky Industrial CyberSecurity for Networks Console.

Viewing security policy properties

To view the properties of a security policy:

1. In the **Manage security policy** menu in the Console window, select **Properties**.

   The **Security policy properties** window is displayed on the screen. The window displays information about the security policy that is currently open in the Console, and information about the security policy that is applied on the Server.

2. View the security policy properties and click **OK** to close the window.

Changing the name of a security policy

You can rename the security policy that is open in the Application Console. If you want to rename the security policy that is running on the Server, you need to load the security policy from the Server, rename it in the Console, and then apply it on the Server.

To change the security policy name:

1. In the **Manage security policy** menu in the Application Console window, select the **Properties** option.

   The **Security policy properties** window is displayed on the screen.

2. In the **Name** field, enter the new name for the security policy and click **OK**.

   The new security policy name will be displayed in the title of the Application Console window.

3. Save the security policy.

About the security policy conversion tool

The security policy conversion tool known as config_converter is intended for converting security policies that were created in Kaspersky Industrial CyberSecurity for Networks version 2.8 so that they can work in the current version of the application.

The config_converter tool is located in the Kaspersky Industrial CyberSecurity for Networks installation directory: /opt/kaspersky/kics4net/bin/.

To launch the config_converter tool use the following command line parameters:

- `--cfg-version` – version of the application in which the original security policy was created.

  Version 2.8 is the default version.

- `-i` – path to the folder with the original security policy. This is a required parameter.

- `-o` – the path to the directory in which the converted security policy will be located. This is a required parameter.

  If the specified directory does not exist, it will be created automatically.

- `-F` – automatically overwrite files in the folder with the converted security policy.

  If the `-F` parameter is set, prior to conversion the config_converter tool will automatically delete all files in the folder in which the converted security policy will be placed.

  If the `-F` parameter is not set, the config_converter tool will ask whether you want to overwrite the files in the directory in which the converted security policy will be located. If you specify the `No` option, conversion will not be performed.

- `-h` – display brief Command Line Help.

- `-l` – language of the config_converter tool interface. The default language is Russian. To use English, you need to specify `english` for the parameter.

Converting and importing a security policy

You can use the security policy conversion utility to convert a security policy from the previous version of Kaspersky Industrial CyberSecurity for Networks. After a security policy is converted, you can import it into the current version of the application.

To convert and import a security policy that was created in a previous version of the application:

1. Open the operating system console and go to the opt/kaspersky/kics4net/bin/ folder.
2. Enter the following command in the command line:

   ```
   ./config_converter -i <name of the folder containing the original policy> \
   -o <name of the folder for the converted policy>
   ```

   Example:

   ```
   ./config_converter -i /home/user1/policy1 -o /home/user1/policy2
   ```

   After the config_converter tool is finished, make sure that there is a converted security policy in the specified folder.
3. Open the converted security policy in the Application Console.
4. If necessary, you can also configure the Process Control settings and the registration settings for event types, and then save the security policy.
5. Apply the security policy on Server.

Process Control

In Kaspersky Industrial CyberSecurity for Networks, Deep Packet Inspection is conducted for devices that transmit and receive process parameters and system commands. Various types of devices supported by the application may be used for Process Control.

For Process Control in industrial network traffic, you can use Process Control rules and monitor system commands.

Process Control rule – set of conditions for the values of tags. 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 conditions of a rule are satisfied, an event is registered in Kaspersky Industrial CyberSecurity for Networks. You can specify the desired type of registered event when configuring a Process Control rule.

Monitoring system commands ensures registration of events when transmitted system commands are detected in traffic. When configuring the settings of process control devices, you can select the relevant system commands to monitor. This functionality can be used regardless of Process Control rules.

Lists containing Process Control rules and containing devices and tags for Process Control are part of a security policy. Only users with the Administrator role can apply the current security policy on the Server. However, users with the Administrator role and users with the Operator role can both make changes and save the security policy to a folder (including with changed settings for process control).

You can generate a list of Process Control rules and a list of devices and tags for process control in the Kaspersky Industrial CyberSecurity for Networks Console on the **Process Control** tab.

When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, you cannot manage Process Control rules or process control devices.

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
  - Allen-Bradley® ControlLogix®, CompactLogix™ series
  - BECKHOFF® CX series
  - Honeywell C300 for Experion PKS / PlantCruise control systems
  - Honeywell ControlEDGE 900 series
  - Emerson DeltaV MD, MD Plus, MQ
  - Emerson ControlWave series
  - General Electric RX3i
  - 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
  - Yokogawa ProSafe-RS
  - Yokogawa AFV10, AFV30, AFV40
  - PLC with a runtime system for CODESYS V3
  - Prosoft-Systems Regul R500
- Intelligent electronic devices (hereinafter referred to as IED):
  - ABB Relion™ series: REF615, RED670, REL670, RET670
  - General Electric MULTILIN series: B30, C60
  - 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 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
- Devices categorized as network equipment:
  - Moxa NPort IA 5000 series
  - I/O devices that support the following protocols: DCE/RPC, FTP, IEC 60870-5-101, IEC 60870-5-104, Modbus TCP, OPC DA, OPC UA Binary, and the WMI device interaction protocol

For the listed 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
- CODESYS V3 Gateway
- DCE/RPC and protocols based on DCE/RPC (OPC DA and the WMI device interaction protocol)
- DMS for ABB AC 700F devices
- DNP3
- Emerson ControlWave Designer
- Emerson DeltaV
- FTP
- General Electric SRTP
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104

- IEC 61850: GOOSE, MMS (including MMS Reports), Sampled Values
- Mitsubishi MELSEC System Q
- Modbus TCP
- OMRON FINS
- OPC UA Binary
- Siemens Industrial Ethernet
- Siemens S7comm™, S7comm-plus
- Yokogawa Vnet/IP
- Relematika BDUBus
- Modification of the MMS protocol for ABB AC 800M devices
- Modification of the Modbus TCP protocol for devices of Ekra 200 series
- Protocol for interaction of Foxboro FCP270, FCP280 devices
- Protocol for interaction of Moxa NPort IA 5000 series devices
- Protocol for initial setup of Prosoft-Systems devices
- Protocol for data exchange with Emerson ControlWave series devices
- Protocol of devices with Siemens DIGSI 4 system software
- Protocols for interaction of devices in Honeywell Experion PKS / PlantCruise control systems
- Protocols for detection and interaction of Honeywell ControlEDGE 900 series devices

Tree of devices and tags for process control

A tree of devices and tags for process control is a hierarchical structure that displays the links between process control devices (for example, PLCs), their protocols and tags. The tags that are part of this structure can be used in Process Control rules.

The following icons are used for the tree elements:

- ▬ – process control device
- ⚙ – protocol
- 🏷 – tag

Devices and tags for Process Control

A *process control device* is a device that is used to automate the industrial process at an enterprise (for example, a programmable logic controller).

A *tag* is a process parameter transmitted in the industrial network (for example, a controlled temperature). The values of tags are transmitted by devices over specific protocols.

Kaspersky Industrial CyberSecurity for Networks supports the use of various types of devices and protocols for Process Control.

> After installation of the application, the application uses the original modules for processing application-layer protocols based on Deep Packet Inspection technology. You can update protocol processing modules by installing updates.

To describe the logical connections between devices, supported protocols and tags, you need to create a hierarchical tree structure from these elements. You can generate a tree of devices and tags in the following ways:

- Manually add assets, protocols (when adding assets or when changing the settings of assets), and tags.
- Add tags from the detected tag storage.
- Import tags and devices from data files.

After adding tags to the tree, you can specify the necessary tags in Process Control rules.

The application only monitors the values of tags specified in Process Control rules.

You can monitor the values of tags in the table of registered events or view them in online mode in the **Tags** section.

The settings of a process control device or tag are displayed in the Application Console on the **Process control** tab. The settings editor area appears in the lower part of the tab when adding or modifying a process control device or tag.

Settings of Process Control devices

The following settings may be defined for process control devices:

- **Device type** is the type of device from the list of supported device types for Process Control in Kaspersky Industrial CyberSecurity for Networks. The supported types of devices are listed in the drop-down list.
- **Host Name** is the name that is displayed in the list of process control devices.
- **System commands** – settings for tracking system commands for a device.

  The **System commands** bar presents the following elements:

  - The **Total** field displays the total number of system commands for the selected protocols.
  - The **Monitored** field displays the number of monitored system commands that will cause the application to register events if detected.
  - The **Select system command** link opens the **Monitored system commands** window in which you can select the system commands to monitor from the list.

- **Protocol** – the utilized protocol. The drop-down list shows the available protocols for the specified device type whose traffic you can monitor.

  When the Modbus TCP protocol is selected, the **Change the places of machine words in 32-bit values** check box appears on the right of the drop-down list. You can use this check box to enable or disable support for an inverted sequence of machine words in 32-bit data values over the Modbus TCP protocol.

  When the IEC 60870-5-101 protocol is selected, the **Advanced settings** link appears on the right of the drop-down list. This link opens the **Advanced settings** window in which you can configure the following protocol settings:

  - **Two-byte ASDU address**. This check box enables or disables two-byte addressing mode for application service data units (ASDU). If this mode is disabled, one-byte addressing is used.
  - **Originator**. This check box enables or disables the use of an additional byte for the originator's address in a data block ID.
  - **Block size for channel address**. This drop-down list lets you select the number of bytes in a link-level address block.
  - **Block size for object address**. This drop-down list lets you select the number of bytes in an address block of an information object.
- **Address** – depending on the selected protocol, this lets you specify the IP address and port, MAC address of the device, or the domain ID (for the IEC 61850: GOOSE protocol).

You can add additional protocols and addresses for a device by using the **Add protocol** and **Additional address of the device** buttons. To remove additional protocols and addresses, use the × buttons on the left of the names of settings.

Settings of tags

The following settings are available for tags:

- Main settings:
  - **Tag name** – displayed name of the tag.
  - **Data type** – type of tag data.
  - **Description** – additional information about the tag.
  - **Unit of measure** – unit of measurement for the process parameter represented by the tag.
  - **ID** – sequential number of the tag. A tag ID is assigned automatically.
- The following settings determine the boundaries of values depending on the selected tag's data type:
  - **Scalable tag** – determines the tag scaling limits in the fields for entering the minimums and maximums for input and output values.
  - **Maximum string length** – determines the number of characters for a tag with a string data type.
- The following settings determine tag data depending on the protocol:
  - **Area**
  - **Memory area**

- Tag address
- ASDU address
- Block number
- Bit
- Bank number
- Bit count
- Group
- Index
- Local identifiers (LID)
- Runtime identifier (RID)
- DB number
- Application
- POU instance
- Variable offset
- Tag MSD ID
- Project MSD version

In the editor area, the mandatory settings are highlighted.

> To receive data on process parameters from devices that support protocols of the IEC 60870-5-104 standard, the corresponding tag data types must be used in Kaspersky Industrial CyberSecurity for Networks. For information about the correspondence between types of application service data units (ASDU) in protocols of the IEC 60870-5-104 standard and tag data types in Kaspersky Industrial CyberSecurity for Networks, please refer to the Knowledge Base on the Kaspersky website ↗.

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 security policy but are associated with devices and protocols that are presented in the tree of devices and tags for Process Control. The security policy that is running on the Server is used by the application to check detected tags.

Unknown Tag Detection mode

Information about unknown tags is obtained from traffic when the application is operating in Unknown Tag Detection mode. You can enable and disable this mode.

When the application is operating in Unknown Tag Detection mode, 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 Unknown Tag Detection mode for a sufficient amount of time to detect all tags that may be associated with devices and protocols in the security policy. It is recommended to disable this mode after you have added detected tags to the security policy.

Unknown Tag Detection is supported for the following protocols:

- Allen-Bradley EtherNet/IP
- 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
- OPC DA
- OPC UA Binary
- Yokogawa Vnet/IP
- Protocol for data exchange with Emerson ControlWave series devices

Detected tag storage

Tags received from traffic in Unknown Tag Detection mode are saved in the detected tag storage. This storage is intended for temporarily storing information about tags before they are added to a security policy.

Information about tags is not duplicated in storage. If the same tag is detected multiple times in traffic, the date and time of last detection of this tag is updated in the storage.

The detected tag storage has the following limits:

- Storage size – no more than 100 MB
- Number of tags in storage – no more than 100000

When any of the specified limits are reached, the application deletes the oldest tags from storage to save newly detected tags. Tags that were detected before the others are considered to be old tags.

The storage is automatically cleared as tags are added to the security policy.

Enabling and disabling Unknown Tag Detection

You can enable or disable Unknown Tag Detection when connected to the Server through a web browser.

Unknown Tag Detection is disabled by default after the application is installed. It is recommended to enable Unknown Tag Detection after first preparing the application. To prepare the application, you need to add all devices and protocols whose tags you want to detect in traffic to the tree of devices and tags. Devices and protocols are added in the Application Console. You can add devices and protocols manually or import them from data files. After adding devices and protocols, you need to apply the current security policy on the Server.

Only users with the Administrator role can enable and disable Unknown Tag Detection.

To enable or disable Unknown Tag Detection:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Technologies** tab.
3. Use the **Unknown Tag Detection** toggle switch to enable or disable Unknown Tag Detection.
4. After you enable or disable this detection mode, wait for the toggle switch to change to the necessary position (*Enabled* or *Disabled*).

   This process takes some time. The toggle switch will be unavailable during this time.

Adding a process control device

You can add the necessary process control devices in the Application Console.

An **IEC 61850 device** is added by importing tags and devices from data files.

To add a new device for Process Control:

1. Select the **Process control** tab in the Console window.
2. In the **Devices and tags** area, click the **Add device** button.

   The device editor appears in the lower part of the tab.
3. Configure the settings:
   - Select the device type.
   - Enter the device name.
   - Specify one or multiple protocols used for communication with the device.
   - Define the settings of one or multiple addresses for communication with the device.
   - If necessary, edit the settings for monitoring system commands for a device. By default, all system commands except those that are frequently encountered during normal operation of the device are monitored for the specified device protocols.
4. Save the device settings by clicking the **OK** button.

The tree of devices and tags for Process Control displays the device and its associated protocols for monitoring.

Adding tags from the detected tag storage

When adding tags from the detected tag storage, the application automatically arranges the added tags in the tree of devices and tags. Tags are added to the security policy that is open in the Console.

It is possible that not all tags from the detected tag storage will be added to the security policy in the Console. You can add only those tags whose corresponding devices and protocols are available in the security policy. If the security policy in the Console does not contain the device and/or protocol corresponding to the tag from the storage, this tag cannot be added to the security policy.

> If you want to add all tags from the detected tag storage, the security policy loaded to the Console must have the same composition of devices and protocols that were used for unknown tag detection. To do so, for example, you can load the current security policy from the Server to the Console (if the composition of devices and protocols in this security policy has not changed since the detection of unknown tags).

When tags are added, the application sequentially processes the tags that are available in the detected tag storage. Each processed tag is automatically deleted from the storage. The application deletes all processed tags from storage, including those that were added to the security policy and those that were not added.

Users with the Administrator role and users with the Operator role can both add tags from the detected tag storage to the security policy in the Console.

To add tags from the detected tag storage to the security policy in the Console:

1. Start the Application Console.

2. Select the **Process control** tab in the Console window.

3. Click the **Load tags** button. The button is available if the detected tag storage is not empty (a non-zero value is displayed in the **Detected tags** field).

   This starts the process for adding tags and opens the **Add detected tags** window. After the process of adding tags is complete, the window displays information about the number of detected tags in the storage, and information about the number of tags added to the security policy.

   > You can interrupt the process of adding tags by clicking the **Cancel** button (this button is displayed until the process completes). If you do so, the security policy will contain only the added tags that were processed before you canceled the process. Unprocessed tags will not be removed from the detected tag storage.

4. Close the **Add detected tags** window.

   The added tags are displayed in the tree of devices and tags on the **Process control** tab. You can change the parameters of added tags and specify these tags in Process Control rules.

After adding tags from the detected tag storage, it is recommended to apply the security policy on the Server and disable Unknown Tag Detection.

If you have finished adding tags but do not apply the security policy on the Server and Unknown Tag Detection is still enabled, the tags that were added to the security policy may be detected again as new tags and sent to the tag storage. This happens because the application only checks whether detected tags are present in the security policy that is being applied on the Server. However, when adding tags from the detected tag storage, the application checks whether they are present in the security policy that is loaded in the Console (not the security policy on the Server). If the added tags are already found in the security policy in the Console, these tags are not duplicated in the policy.

Manually adding a tag

To manually add a new tag:

1. Select the **Process control** tab in the Console window.

2. In the tree of devices and tags, select the device and its protocol for which you want to add a tag. You must select a protocol in which the transmission of tags is supported. You can also select one of the available tags for the protocol.

   After selecting a protocol (or one of the tags of this protocol), the **Add tag** button becomes active. The button will be inactive if you have selected a protocol in which the transmission of tags is not supported (for example, the FTP system protocol).

3. Click the **Add tag** button.

   The tag editor appears in the lower part of the tab.

4. Configure the settings:

   - Specify the required settings whose names are distinguished by font (for example, the tag name and data type).

   - If necessary, specify the other settings that are available for the tag depending on the protocol and the selected data type (for example, the unit of measurement and scaling limits).

5. Save the tag settings by clicking the **OK** button.

The tree of devices and tags will display the new tag for the selected protocol.

Editing the settings of a process control device or tag

To change the settings of a process control device or tag:

1. Select the **Process control** tab in the Console window.

2. In the tree of devices and tags, select the element whose settings you want to change.

3. Click **Edit** in the lower-right corner of the tab.

4. If a tag is selected, you will be prompted to continue. If this is the case, confirm that you want to modify tag settings.

   The device editor or tag editor appears in the lower part of the screen.

5. When configuring the settings for a device:

   a. Enter the device name.

   b. Specify one or multiple protocols used for communication with the device.

   c. Define the settings of one or multiple addresses for communication with the device.

   d. If necessary, edit the settings for monitoring system commands for a device.

6. When configuring the settings for a tag:

   a. Specify the required settings whose names are distinguished by font (for example, the tag name and data type).

   b. If necessary, specify the other settings that are available for the tag depending on the protocol and the selected data type (for example, the unit of measurement and scaling limits).

7. Save changes by clicking the **OK** button.

Removing a process control device or tag

To remove a process control device or tag:

1. Select the **Process control** tab in the Console window.

2. In the tree of devices and tags, select the element that you want to remove.

3. Click the **Remove** button.

4. Confirm removal of the device or tag.

   The selected item will be removed from the list.

Searching tags

You can perform a search for tags based on the values of any column.

To filter the found tags, you can select one of the following filter settings:

- All tags created in the current security policy

- Tags used in any Process Control rules

- Tags used in the selected Process Control rule

To find the relevant tags:

1. In the upper-right corner of the **Devices and tags** area, enter your search query into the **Tag search** field. To search by tag ID, enter `id:` in the search field and then enter the desired IDs separated by a space (for example, `id: 3 52 675`). The search is initiated as you enter characters.

The tree of devices and tags displays the tags that meet the search criteria. The found tags will be displayed together with the devices and protocols associated with those tags.

2. If necessary, select the necessary filter setting in the **Show tags** drop-down list:

   - **All** – to display all found tags.
   - **In rules** – to display the tags found in all existing Process Control rules.
   - **In the current rule** – to display the tags found only for the selected Process Control rule.

   The tree of devices and tags will display the items that match the filtering criterion.

3. If you selected the **In the current rule** filter setting and you want to display the tags found in another Process Control rule, select the relevant rule in the table of Process Control rules.

Importing tags and process control devices from data files

You can add tags and process control devices that were previously created using other systems (for example, SCADA) to the security policy of Kaspersky Industrial CyberSecurity for Networks. Kaspersky Industrial CyberSecurity for Networks imports tags and process control devices from data files.

To import custom tags and process control devices into Kaspersky Industrial CyberSecurity for Networks using data files:

1. Select the **Process control** tab in the Console window.

2. Click the **Import** button.

   The screen shows the window in which you can select the folder containing the data files to be imported.

3. Specify the path to the folder storing the data files.

4. Click the button for selecting a folder.

   If the list of devices and tags is not empty, in the window that appears, specify the method for importing: **Add** or **Replace**. When the **Add** option is selected, the imported devices will be added to the list of existing devices. When the **Replace** option is selected, existing devices in the list will be replaced by the imported devices.

5. Confirm the data import by clicking **OK**.

The imported process control devices and their associated protocols and tags will appear in the list on the **Process control** tab.

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 device 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).

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 available parameters for this event type in the Application Console on the **Configure events** tab.

You can view information about registered events when connected to the Server through a web browser.

To configure monitoring of system commands for a device:

1. Select the **Process control** tab in the Console window.

2. In the list of devices and tags, select the device for which you want to configure monitoring of system commands.

3. Click the **Edit** button.

   The device editor appears in the lower part of the window.

4. In the device editor area, in the **System commands** line, click the **Select system command** link.

   You will see the **Monitored system commands** window containing a list of system commands that can be monitored.

   > The list of monitored system commands depends on the specified protocols for the device. If the necessary system commands are absent from the list, close the **Monitored system commands** window and add all missing protocols that could be used by the device to the device settings.

5. In the **Monitored system commands** window, select the check boxes next to the system commands that you want to monitor.

6. Click **OK**.

7. Save changes by clicking the **OK** button.

8. Apply the security policy.

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
Prosoft-Systems Regul R500, PLC with a runtime system for CODESYS V3	CODESYS V3 Gateway	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET

EKRA 200 series	Modbus TCP for devices of Ekra 200 series	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:

- Network Control is enabled in monitoring mode and Command Control technology is applied.
- The table of Network Control rules does not contain any rules for Command Control technology that allow system commands with default passwords. For example, such rules may be automatically created in Network Control learning mode. If the table of Network Control rules contains rules that allow system commands with default passwords, it is recommended to switch these rules to inactive state.
- For the relevant assets, tracking of system commands with default passwords is enabled.

Process Control rules

The application can employ the following Process Control rules:

- Rules with defined conditions
- Rules with Lua scripts

You can combine Process Control rules into groups to logically organize rules based on user-defined attributes (for example, rules related to specific devices can be put into different groups). You can form a hierarchical structure of groups and rules nested within them. Up to eight nesting levels are supported.

The following icons are used for the tree elements:

- ▤ – group.
- ◢ – rule with defined conditions.
- □ – rule with a Lua script.

About Process Control rules

A Process Control rule with defined conditions consists of a set of conditions for tag values. You can bind multiple conditions with the logical operators AND/OR. When using multiple conditions, you can specify the priorities that will determine the order in which conditions in the rule are applied. An event is registered when the conditions defined in a rule are satisfied. You can select the necessary event type for a rule. A rule can contain no more than eight conditions.

A rule containing a Lua script consists of a script in the Lua language containing a description of the algorithm used for event registration.

If you are using Lua scripts to create Process Control rules, you can use a *global script*, which is a Lua script in which global variables and Lua functions are initialized. You can use these global variables and functions in a Lua script for any particular rule. A specified global Lua script is automatically executed when the security policy is applied. When a security policy is created, the global Lua script is empty and does not contain executable code. A security policy can have only one global Lua script, which can be viewed and modified when working with any rule containing a Lua script.

The settings of a Process Control rule are displayed in the editor area that appears under the rule list when adding or modifying a rule.

In the left part of the rule editor area, you can configure the following settings:

- Rule name and description.
- For rules in which conditions are defined for the values of tags, you can configure the settings of conditions whose violation will cause an event to be registered. For information about conditions, please refer to the Types of conditions for the Process Control rules section.
- For rules consisting of a Lua script, you can configure the type of Lua script (**Rule script** or **Global script**) and the text of the Lua script. When creating a rule script, the entry field displays a Lua script template with brief comments. You can use the help button above the script entry field to open a window containing detailed comments for creating a script. For information about the applied functions and variables, please refer to the Functions and variables for a Lua script section.

In the right part of the rule editor area, you can configure the type of event that will be registered when the rule conditions are satisfied.

You can use the **Event** drop-down list to select an existing event type or add a new type. The following control buttons are located next to the drop-down list:

- ✎ – edits the selected event.
- + – adds a new event.

An event type in the rule editor area uses the same event type settings that are provided on the Configure events tab.

Rules with defined conditions for tag values

In a Process Control rule that defines conditions for the values of tags, you need to specify the type of each condition. Each type has a certain number of additional settings that also include tags.

You can specify the types of conditions when performing the following actions:

- Creating a Process Control rule with settings of conditions

To create a rule:

1. Select the **Process control** tab in the Console window.
2. If the list of Process Control rules contains groups, select the group to which you need to move the new rule. You can select the group itself or one of the existing rules from the group.
3. Click the **Add rule** button.
   The rule editor appears in the lower part of the tab.
4. Perform the following actions:
   a. Enter the rule name and description.
   b. Define the conditions.
   c. Select or configure the type of registered event.
5. Click **OK**.
   The new rule appears in the list.
6. To apply the changes, apply the security policy.

The application Server will begin to register events when the rule conditions are fulfilled.

- Editing a Process Control rule with settings of conditions ?

To edit a rule:

1. Select the **Process control** tab in the Console window.
2. In the list of Process Control rules, select the rule that you want to edit.
3. Click the **Edit** button.
   The rule editor appears in the lower part of the tab.
4. Perform the following actions:
   a. Enter the rule name and description.
   b. Define the conditions.
   c. Select or configure the type of registered event.
5. Click **OK**.
6. To apply the changes, apply the security policy.

The application Server will begin to register events based on the changes made to the rule.

In the drop-down list of condition types, you can select one of the following options:

- **Equal to** – the value of the controlled tag is equal to the specified value.
  Two parameters are used in this type of condition:
  - Parameter 1: controlled tag of the int, bool, string type.
  - Parameter 2: specified value (constant or tag).
- **Does not equal** – the value of the controlled tag is not equal to the specified value.
  Two parameters are used in this type of condition:
  - Parameter 1: controlled tag of the int, bool, string type.
  - Parameter 2: specified value (constant or tag).

- Less than – the value of the controlled tag is less than the specified minimum permissible value.

  Two parameters are used in this type of condition:

  - Parameter 1: controlled tag of the int, float type.
  - Parameter 2: minimum permitted value (constant or tag).

- Greater than – the value of the controlled tag is greater than the specified maximum permissible value.

  Two parameters are used in this type of condition:

  - Parameter 1: controlled tag of the int, float type.
  - Parameter 2: maximum permitted value (constant or tag).

- Deviation exceeds allowance – if the controlled tag value differs from the specified value by more than the value of the allowance parameter.

  Three parameters are used in this type of condition:

  - Parameter 1: controlled tag of the int, float type.
  - Parameter 2: specified value (constant or tag).
  - Parameter 3: allowance as a percentage of the specified value (constant – an unsigned number in the range from 0.001 to 100).

- Out of range – the value of the controlled tag is outside of the specified range.

  Three parameters are used in this type of condition:

  - Parameter 1: controlled tag of the int, float type.
  - Parameter 2: lower boundary of the range (constant or tag).
  - Parameter 3: upper boundary of the range (constant or tag).

- Value has changed – the value of the controlled tag is changing.

  One parameter is used in this type of condition: controlled tag of any type.

- Tag bit equals – the value of the monitored bit in the controlled tag is equal to the specified value.

  Three parameters are used in this type of condition:

  - Parameter 1: controlled tag of the int or unsigned int type.
  - Parameter 2: 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).
  - Parameter 3: value of the monitored bit in the tag (specified as one of two integers: zero or one).

- Detection – the controlled tag was detected in the traffic being monitored.

  One parameter is used in this type of condition: controlled tag of any type.

- Change exceeds allowance – the change in the value of the controlled tag exceeds the allowance relative to the previously registered value of the tag.

  Two parameters are used in this type of condition:

    - Parameter 1: controlled tag of the int, float type.

    - Parameter 2: allowance as a percentage of the previous value (constant – an unsigned number in the range from 0.001 to 100).

- **Tag bit has changed** – the value of the monitored bit in the controlled tag is changed.

  Two parameters are used in this type of condition:

    - Parameter 1: controlled tag of the int or unsigned int type.

    - Parameter 2: 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).

To define a tag for a setting, you can select the relevant tag in the drop-down list or drag the tag from the **Devices and tags** list.

In the drop-down list to the right of the field containing the selected tag, you can select which most recent value of the tag is used in the rule. The following options are provided:

- **Read** – the most recent tag value intercepted when reading the tag from the device.

- **Write** – the most recent tag value intercepted when writing the tag to the device.

- **Read and write** – the most recent tag value intercepted when reading or writing the tag.

You can define multiple conditions in a Process Control rule. To apply multiple conditions, you can select logical operators (AND / OR) and specify the priorities of conditions by using parentheses in logical expressions. You can add a condition by clicking the **Add condition** button. To remove an additional condition, use the x button on the left of the condition.

Rules using Lua scripts

The function in a rule's Lua script described in the Lua language 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.

You can change functions in Lua scripts when performing the following actions:

- Creating a Process Control rule with a Lua script

To create a Lua rule script:

1. Select the **Process control** tab.

2. If the list of Process Control rules contains groups, select the group to which you need to move the new rule. You can select the group itself or one of the existing rules from the group.

3. Click the **Add Lua script** button.

   The Lua script editor appears in the lower part of the tab.

4. In the Lua script editor above the script entry field, select the **Rule script** option.

5. Perform the following actions:

   a. Enter the rule name and description.

   b. Enter the code of the script in the Lua language.

      The script entry field displays the template for a Lua language function with brief comments. Click the help button above the script entry field to open the window containing detailed comments for creating a script.

   c. Select or configure the type of registered event.

6. Click **OK**.

   The new Lua script appears in the list.

7. To apply the changes, apply the security policy.

- ## Creating or editing a global Lua script ?

To edit a global Lua script:

1. Select the **Process control** tab.

2. Open the Lua script editor. To do so, you can use one of the following methods:

   - If the list of Process Control rules does not contain rules containing Lua scripts, create a new rule with a Lua script. To do so:

     - If the list of Process Control rules contains groups, select the group in which the rule containing a Lua script will be created. You can select the group itself or one of the existing rules from the group.

     - Click the **Add Lua script** button.

   - If the list of Process Control rules contains at least one rule that has a Lua script:

     - Select any rule containing the Lua script.

     - Click the **Edit** button.

3. In the Lua script editor above the script entry field, select the **Global script** option.

4. In the script entry field, enter the code of the script in the Lua language.

   To open the window containing comments on creating a global script, click the help button above the script entry field.

5. Click **OK**.

6. To apply the changes, apply the security policy.

The defined global variables and functions of a global Lua script can be used when creating or editing rules containing Lua scripts.

- ## Editing a Lua script in a Process Control rule ?

To edit a Lua rule script:

1. Select the **Process control** tab.
2. In the list of Process Control rules, select the rule with the Lua script that you want to edit.
3. Click the **Edit** button.
   The Lua script editor appears in the lower part of the tab.
4. In the Lua script editor above the script entry field, select the **Rule script** option.
5. Perform the following actions:
   a. Enter the rule name and description.
   b. Enter the code of the script in the Lua language.
      Click the help button above the script entry field to open the window containing detailed comments for creating a script.
   c. Select or configure the type of registered event.
6. Click **OK**.
7. To apply the changes, apply the security policy.

The application Server will begin to register events based on the changes made to the rule.

Tags are described in the function code by an expression in the following format:

`X = tag'tag_name'[.R/.W/.RW]`,

where the following modifier values are used: `.R` – tag is intercepted when reading the tag from the device, `.W` – tag is intercepted when writing the tag to the device, `.RW` – any most recent value of the tag. You are not required to specify a modifier. If a modifier is not specified, any most recent tag value is used.

When creating a rule using a Lua script, you can use additional variables with a user-defined name and value.

The following function is used to add a variable:

```
_AddEventParam('parameter_name', parameter_value)
```

You can use the added variable in the settings of custom event types. The added variable may be used in the format `$extra.<parameter_name>.`

You can use functions for adding a record 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:

- `_WriteCriticalLog(function_argument)` creates a log record with the *Critical* level.
- `_WriteErrorLog(function_argument)` creates a log record with the *Error* level.
- `_WriteWarningLog(function_argument)` creates a log record with the *Warning* level.
- `_WriteInfoLog(function_argument)` creates a log record with the *Informational* level.
- `_WriteDebugLog(function_argument)` creates a log record with the *Debug* level.
- `print(function_argument1, function_argument2,…)` creates a log record with the *Debug* level that may contain multiple arguments of the function. 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 log level set for the process in the Settings of Server and sensors window.

Creating a group in the list of Process Control rules

To create a group:

1. Select the **Process control** tab.
2. If you need to add a new group into an existing group, select the group that will serve as the parent group.
3. Click the **Add group** button.

   The **Group name** window appears on the screen.
4. Enter the group name.
5. Click **OK**.

   The new group appears in the list.
6. If necessary, move the group in the list.

Moving an item in the list of Process Control rules

To move a list item:

1. Select the **Process control** tab.
2. In the list of Process Control rules, select the item that you want to move.
3. Use the mouse to drag the item to the necessary place in the list.

Renaming an item in the list of Process Control rules

To rename a list item:

1. Select the **Process control** tab.
2. In the list of Process Control rules, select the item that you want to change.
3. Click the **Edit** button.
4. You will see the editor area (if a rule is selected) or the **Group name** window (if a group is selected).
5. Enter the new name of the item.
6. Click **OK**.

Removing an item from the list of Process Control rules

To remove a list item:

1. Select the **Process control** tab.
2. In the list of Process Control rules, select the item that you want to remove.
3. Click the **Remove** button.

   A window with a confirmation prompt opens.
4. Click **Yes**.

The item will be removed from the list.

Searching Process Control rules

You can search Process Control rules and groups based on values in the **Name** and **Description** columns.

To find the relevant Process Control rules and groups:

1. In the upper-right corner of the **Process Control rules** area, enter the search query into the **Rule search** field. The search is initiated as you enter characters.

   The list of Process Control rules displays the rules and groups that meet the search criteria.
2. If you want to exclude groups from search results, clear the **Show groups** check box.

Highlighting tags used in Process Control rules

To view the tags used in Process Control rules, you can highlight the tags that are associated with the selected rules. Depending on the selected item in the list of Process Control rules, the application highlights the following tags:

- Tags of the selected Process Control rule.
- Tags of rules of the selected group.

To highlight listed tags that are used in the selected rule or rules of the selected group:

Select the relevant item in the list of Process Control rules (group or individual rule).

In the **Devices and tags** tree, all tags associated with the selected item will be highlighted. Tags are highlighted in light green. To display the highlighted tags on the screen, expand the corresponding nodes of the tree and, if necessary, vertically move the slider on the right of the tree.

Configuring events

In the Console, you can configure the types of registered events of Kaspersky Industrial CyberSecurity for Networks. When configuring them, you can create, modify, or remove event types, and configure the transmission of events to recipient systems.

The list of types of registered events is displayed in the Kaspersky Industrial CyberSecurity for Networks Console on the **Configure events** tab. Each event type corresponds to one of the technologies used by the application.

> When you connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser, you cannot work with the list of event types.

The list of event types is part of the security policy. Only users with the Administrator role can apply the current security policy on the Server. However, users with the Administrator role and users with the Operator role can both make changes and save the security policy to a folder (including with changed settings for event types).

The list of event types contains system event types and custom event types. *System event types* are created by the application during installation and cannot be deleted from the list. The application uses system event types to register primary events based on Deep Packet Inspection technology and to register any events based on other technologies. You can create additional event types for Deep Packet Inspection and External technologies. These event types are called *custom event types*.

For custom event types, you can delete and modify settings, and select recipients. For system event types, you can select recipients and modify individual registration settings.

> You can use custom event types to configure receipt of events from external systems. To do so, in the Console, you need to specifically create event types to be received from an external system. When an event type is created, it is assigned a unique number (this number is saved as the value of the **Code** setting). Then, in the external system, you need to configure the transmission of events to the application using Kaspersky Industrial CyberSecurity for Networks API methods. When sending an event to Kaspersky Industrial CyberSecurity for Networks, the external system will specify the event type identifier defined by the **Code** setting. Using this identifier, the Kaspersky Industrial CyberSecurity for Networks Server will determine the event type and register it as an event based on External technology.

The following settings are available for event types:

- **Code** – unique event type number that will be displayed in the list of event types on the **Configure events** tab. In the table of registered events, the event type identifier is displayed in the **Event type** column. The event type identifier is automatically assigned by the application when the event type is created. This setting cannot be changed.
- **Severity** – importance level that will be specified for the event when it is registered: *Critical*, *Warning*, or *Informational*. This setting can be changed only for custom event types.
- **Technology** – technology used for event registration. This setting is accessible only for custom event types. You can specify Deep Packet Inspection or External technology.
- **Title** – text of the event title. It is displayed in the list of event types on the **Configure events** tab. In the table of registered events, the title of the event type is displayed in the **Title** column. The titles of event types are also displayed in the **Events** block in the **Dashboard** section of the application web interface. This setting can be changed only for custom event types.
- **Description** – additional text that will be displayed in the table of registered events in the **Description** column. This setting can be changed only for custom event types.

- **Keep traffic** – check box that lets you enable or disable automatic saving of traffic that was registered in the system before and after registration of the event. Traffic is saved in the application database. If the automatic saving of traffic is enabled, you can configure the settings for saving traffic by clicking the **Configure** link.

  > 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.

- **Event regenerate timeout** – maximum period of time after which an event is allowed to be registered again. If the conditions for event registration are repeated again before the specified time period elapses, the 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.

  > For registered events, the event regenerate timeout may occur earlier than the specified period. Re-registration of an event is allowed if the *Resolved* status was assigned to the event, and if the computer performing Server functions was restarted.

The texts of titles and descriptions in the settings of event types may contain variables. When registering events, the Server inserts the current values of the variables.

You can view the registered events when connected to the Server through a web browser.

Grouping event types

You can group the list of event types based on the following criteria:

- By technology. Within each technology, items are grouped by their importance level (severity).
- By severity. Within each importance level, items are grouped by technology.

By default, grouping of event types is disabled.

To group event types:

In the toolbar of the **Configure events** tab, select the necessary grouping mode in the **Group** drop-down list.

Searching for event types

You can search codes and titles in the list of event types.

To find the relevant type of events:

In the toolbar of the **Configure events** tab, enter your search query into the **Search for event types** field. The search is initiated as you enter characters.

The list of event types will display the elements that meet the search criteria (the values of the **Description** setting in event types are not taken into account during the search).

Creating event types

You can create custom event types for Deep Packet Inspection and External technologies.

Created event types for External technology can be used to receive events in Kaspersky Industrial CyberSecurity for Networks from external systems.

To create an event type:

1. On the **Configure events** tab, click the **Add** button.

   The settings editor area appears in the lower part of the **Configure events** tab.

2. Perform the following actions:

   a. Assign the event severity: *Critical*, *Warning*, or *Informational*.

   b. Select the event registration technology.

   c. Enter the event title.

   d. Enter the event description.

   e. If necessary, enable and configure saving of traffic.

   f. If necessary, change the event regenerate timeout.

3. Click **OK**.

The new event type will appear in the list.

You can select a new event type when creating a Process Control rule on the **Process control** tab. Events of the new type will be registered after the security policy is applied on the Server.

Changing event types

To change the event type:

1. On the **Configure events** tab, select the relevant event type and click the **Edit** button.

   A warning window opens.

2. Click **OK**.

   The settings editor area appears in the lower part of the **Configure events** tab.

3. Perform the following actions:

   a. Assign the event severity: *Critical*, *Warning*, or *Informational* (available only for custom events).

   b. Enter the event title (available only for custom events).

   c. Enter the event description (available only for custom events).

   d. Configure the saving of traffic.

   e. Configure the event regenerate timeout.

4. Click **OK**.

   The change to the severity or title of the event will be displayed in the list of event types.

Configuring automatic saving of traffic during event registration

When creating or editing event types, you can enable the automatic saving of traffic for events when they are registered. If saving of traffic is enabled, the network packet that invoked event registration as well as packets before and after event registration are saved in a database. 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, 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 the saving of traffic is enabled for incidents (meaning for system types of events assigned the codes 8000000000, 8000000001, 8000000002 or 8000000003), the application saves traffic for all embedded events of the incident when an 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 types of events 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.

Enabling and configuring the saving of traffic for incidents is sufficient for one of the event types with codes 8000000000, 8000000001, 8000000002 or 8000000003. The application automatically applies the changes made to one of these event types to the remaining three types.

To configure the settings for saving traffic for an event type:

1. In the event type settings editor, select the **Keep traffic** check box.

2. Open the **Save event traffic** window by clicking the **Configure** link.

3. In the **Save event traffic** window, configure the saving of traffic before event registration. To do so, specify the necessary values in the **Packets before event** and/or **Milliseconds before event** 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.

4. Configure the saving of traffic after event registration. To do so, specify the necessary values in the **Packets after event** and/or **Milliseconds after event** 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.

5. Click **OK**.

Deleting event types

You can delete custom event types that are not associated with Process Control rules. You cannot delete system event types.

To delete the event type:

1. On the **Configure events** tab, select the event type to delete.

2. Click the **Remove** button.

   You will be prompted to confirm deletion.

3. In the prompt window, click **OK**.

About transmission of events to recipient systems

When configuring event types, you can specify the recipient systems to which the registered events will be relayed. These recipient systems are called *recipients*. Kaspersky Industrial CyberSecurity for Networks can relay event information to several recipients simultaneously.

Kaspersky Industrial CyberSecurity for Networks can relay event information to the following recipients:

- SIEM server
- Syslog server
- Email
- Kaspersky Security Center

To relay events to Kaspersky Security Center on the Kaspersky Industrial CyberSecurity for Networks Server, you must add the capability for application interaction with Kaspersky Security Center. You can add this functionality during installation or reinstallation of Kaspersky Industrial CyberSecurity for Networks.

> To relay events to other recipient systems, you do not need to add the capability for application interaction with Kaspersky Security Center.

The following settings are available for recipients:

- **Recipient name** – the name that is displayed in the column header on the **Configure events** tab.
- **Recipient type** – the selected type of recipient. Depending on the selected type, you can configure the following additional settings:
  - For a SIEM server and Syslog server: address and port of the server.

    > The contents and order of information about events relayed to SIEM server and Syslog server recipients may differ from the contents and order of information displayed in the events table.

  - For email: notification settings.

    A *notification* is an email message that contains events of Kaspersky Industrial CyberSecurity for Networks. The following settings are applied to notifications:

    - Address of notification sender.
    - Address of notification recipient. Multiple addresses must be separated by commas.
    - Subject of notification.
    - An event template is a text description template for events in a notification. A template determines the content and order in which information is displayed about each event in a notification. A template is generated using variables.
    - Text of notification. In the notification text, you can specify the `$events` variable, which is replaced by a list of lines containing information about events when the Server creates a notification. Each line corresponds to an event template with the current values of variables.
    - Number of notifications per day. Determines the maximum number of notifications per day, starting at 0:00 hours in the time zone of the Server. If there are more notifications, recipients are sent an email message stating that the maximum number of event notifications has been exceeded. If this is the case, new notifications will not be sent until the end of the current day.
    - Quantity of events in each notification. Determines the maximum number of events whose information can be placed into one notification. If there are more events, two or more notifications with this same limit are created (within the daily limit).
  - For Kaspersky Security Center: quantity of relayed events per day. This setting determines the maximum number of relayed events per day, starting at 0:00 hours in the time zone of the Server. If there are more events to relay, the other events registered before the end of the current day are not sent to Kaspersky Security Center.

The settings that determine the maximum number of relayed events are applied to events that are registered in Kaspersky Industrial CyberSecurity for Networks. If information about multiple network interactions is provided in a specific event, this event is converted into separate event records for a recipient (with one event for each network interaction). For this reason, the list of events for a recipient may contain more events than specified by the parameter that determines the maximum number of events.

Adding a recipient

To add a recipient:

1. Select the **Configure events** tab in the application Console.
2. Click the **Specify recipient** button.

   The **Recipients** window appears on the screen.
3. Perform the following actions:

   a. Enter the recipient name.

   b. Select the recipient type and define the remaining settings for sending events.
4. Click **OK**.

The **Configure events** tab will display a column in whose title the name of the added recipient will be specified.

Changing the recipient settings

To edit recipient settings:

1. Select the **Configure events** tab in the application Console.
2. Click the title of the column with the name of the recipient whose settings you want to change.

   The **Recipients** window appears on the screen.
3. If necessary, do the following:

   a. Enter the recipient name.

   b. Define the settings for sending events.
4. Click **OK**.

If you changed the name of a recipient, the new name is displayed in the column header on the **Configure events** tab.

Configuring the transmission of events to recipient systems

To configure the transmission of Kaspersky Industrial CyberSecurity for Networks events to recipient systems:

1. Select the **Configure events** tab in the application Console.

2. Make sure that the list of event types displays the recipients to whom you want to relay application events.

   If the relevant recipient is missing, add it to the list.

3. In the lines containing event types or groups (subgroups) of event types, select the check boxes for the relevant recipients.

The application will send the selected types of events to the recipients after the security policy is applied on the Server.

Removing a recipient

To remove a recipient:

1. Select the **Configure events** tab in the application Console.

2. Click the title of the column containing the name of the recipient that you want to remove.

   The **Recipients** window appears on the screen.

3. Click the **Remove recipient** button.

Kaspersky Industrial CyberSecurity for Networks event configuration variables

You can use Kaspersky Industrial CyberSecurity for Networks variables in the following cases:

- When creating and modifying custom event types.

- When configuring the settings for relaying events by email.

In place of the specified variables, the Server automatically inserts the current values of settings when registering or relaying an event.

In the settings of custom event types, you can use the following variables for the **Title** and **Description** entry fields:

- `$communications` – lines of the description of network interactions (one line for each network interaction) indicating the protocol and addresses of the network packet source and destination.

- `$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).

- `$Event_type_id` – code of the event type.

- `$monitoring_point` – name of the monitoring point whose traffic invoked registration of the event.

- `$occurred` – date and time of event registration.

- `$protocol` – name of the application-level protocol that was being monitored when the event was registered.

- `$src_address` – address of the network packet source (depending on the data available in the protocol, this can be an IP address, port number, MAC address and/or other address data).
- `$tags` is the list of all names and values of tags participating in the Process Control rule.
- `$technology_rule` – name of the Process Control rule by which the event was registered.
- `$top_level_protocol` – name of the top-level protocol.
- `$extra.<paramName>` – additional variable added using the AddEventParam function for an external system or Lua script.

In the Email recipient settings, you can use the following variables for the **Event template** entry field:

- `$closed` – date and time when the *Resolved* status was assigned or the date and time of the event regenerate timeout (for events that are not incidents), or the date and time of registration of the last event included in the incident (for incidents).
- `$communications` – lines of the description of network interactions (one line for each network interaction) indicating the protocol and addresses of the network packet source and destination.
- `$count` – number of times an event or incident was triggered.
- `$description` – event description.
- `$Event_id` – unique ID of the registered event.
- `$Event_type_id` – code of the event type.
- `$monitoring_point` – name of the monitoring point whose traffic invoked registration of the event.
- `$occurred` – date and time of event registration.
- `$severity` – importance level of the event.
- `$technology` – technology associated with the event.
- `$technology_rule` – name of the rule by which the event was registered.
- `$title` – event title.

In the Email recipient settings, for the **Text of notification** entry field, you can use the `$events` variable only. The variable is replaced by a list of lines containing information about events. Each line will correspond to an event with the current values of variables from the **Event template** field.

To insert a variable into the entry field:

1. Set the cursor in the necessary position of the entry field in which you want to use the variable.
2. Click the **Add variable** button or enter the $ character (the $ character needs to be separated from the preceding word by a space).

   The entry field next to the cursor will display a drop-down list of available variables.
3. Select the relevant variable from the drop-down list.

The variable will be added to the entry field and will be distinguished by a special font.

Asset management

Kaspersky Industrial CyberSecurity for Networks lets you monitor devices connected to an industrial network. An assets table is created for the purpose of asset management in the application.

The assets table contains asset information that was manually provided or obtained automatically during traffic analysis.

Only information that can be identified during traffic analysis can be automatically obtained and updated (for example, address information of an asset). For asset 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 asset category if the currently defined category differs from the one that is determined automatically).

Some information must be specified manually because it cannot be automatically updated. For example, you can save specific information about assets in the table, and add absent criteria for sorting and filtering assets. You can also use manually defined information to arrange assets in various groups in the group tree, or filter and search for assets based on asset labels.

Information from the assets table is stored on the Server and is independent of the security policy that is loaded in the Console or applied on the Server. However, process control devices saved in a security policy are automatically added to the assets table after the policy is applied on the Server (or the address information of previously added assets is updated).

You can view and edit information about assets in the **Assets** section of the Kaspersky Industrial CyberSecurity for Networks web interface. You can also view information about the interactions between assets and perform various actions with assets when working with the network map.

Asset Management modes and methods

Kaspersky Industrial CyberSecurity for Networks employs the following methods:

- Asset activity detection. This method lets you monitor the activity of assets in industrial network traffic based on the obtained MAC- and/or IP addresses of assets.
- Asset Information Detection. This method lets you automatically obtain and update information about assets based on received data about the interactions of assets.
- 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.

You can enable and disable the use of individual asset management methods.

The following modes are available for asset management methods:

- Learning mode. This mode is intended for temporary use. In this mode, all assets whose activity is detected in traffic are considered to be authorized by the application. You can enable learning mode only for the asset activity detection method. The Asset Activity Detection method can be applied together with the Asset Information Detection and PLC Project Control methods.

- Monitoring mode. This mode is intended for continual use. In this mode, when activity of assets is detected, the application considers only those assets that have been assigned the *Authorized* status as authorized.

In learning mode, the application assigns the *Authorized* status to all detected assets. The application does not register events when it detects activity of assets or when asset information is automatically updated.

Asset management learning mode must be enabled for a sufficient amount of time to detect the activity of new 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 ranging from one to several days to detect the activity of all new devices.

In monitoring mode (when the asset activity detection method is enabled), the application assigns the *Unauthorized* status to all devices that have showed activity and are either unknown to the application or are assets that have the *Archived* status. The application assigns the *Archived* status to assets that have not shown activity and whose information has not changed in a long time (30 days or more).

When the asset information detection method is enabled, the application automatically updates information about assets. For example, the application can automatically update the name of the operating system installed on an asset as it detects updated data in the traffic of the asset. The application updates data for which automatic updates are enabled in the settings of assets.

To automatically receive information about assets, the application analyzes industrial network traffic according to the *rules for identifying information about devices and the protocols of communication between devices*. These rules are embedded in the application and are applied independent from the security policy loaded in the Console or applied on the Server.

> After installation, the application uses the default rules for identifying information about devices and the protocols of communication between devices. In most cases, these rules generate correct results. However, there can be situations when information is incorrectly identified due to the technical specifics of devices (for example, when identifying the category of some 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.

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 assets with the *Archived* status.
- Automatic change of asset information.
- Detection of read/write operations with projects and PLC project blocks.

> 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/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.

About monitoring read/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:

- Schneider Electric Modicon: M580, M340
- Siemens SIMATIC S7-300, S7-400

To monitor read and write of PLC projects, you are not required to add assets to the list of process control devices. Read and write of PLC projects is monitored for all detected assets of the specified types.

For each asset, 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 an asset, 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 PLC project/block is written:
  - 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 in the Application Console on the **Configure events** tab.

You can view information about registered events when connected to the Server through a web browser.

Selecting the applied methods and changing the Asset Management mode

Only users with the Administrator role can manage asset management modes and methods.

To enable or disable the use of asset management methods:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Technologies** tab.
3. Enable or disable the use of asset management methods by using the following toggle switches:
   - **Asset Activity Detection**
   - **Asset Information Detection**
   - **PLC Project Control**
4. After a method is enabled or disabled, wait for the toggle switch to change to the necessary position (*Enabled* or *Disabled*).

   The process may take some time, during which the toggle switch will be unavailable. Wait for the method to be enabled or disabled.
5. If the asset activity detection method is enabled, select the necessary asset management mode to be applied with the method. To do so, in the drop-down list on the right of the method name, select one of the following values:
   - **Learning** – to apply the method in learning mode.
   - **Monitoring** – to apply the method in monitoring mode.
6. After the mode is selected, wait for the name of this mode to appear in the field of the drop-down list.

   This process may take some time, during which the drop-down list displays the *Changing* status. Wait for the selected mode to be enabled.

Assets table

An assets table is created for the purpose of asset management in the application. All assets in the table are considered to be known to the application.

The assets table has the following limitations on the number of elements:

- The total number of assets with the *Authorized* and *Unauthorized* statuses can be no more than 1000.

  If the maximum number of assets with the *Authorized* and *Unauthorized* statuses is reached, new assets with these statuses are not added to the table. If this is the case, to add a new asset to the table you need to remove one of the previously added assets.

- The number of assets with the *Archived* status can be no more than 1000.

  If the maximum number of assets with the *Archived* status is reached, new assets with this status are added to the table in place of assets that have went the longest without showing any activity.

When the assets table is overfilled, the application displays the appropriate message.

The assets table contains the following information:

- **Name** – name used to represent an asset in the application.
- **Asset ID** – asset ID assigned in Kaspersky Industrial CyberSecurity for Networks.
- **Status** – asset status that determines whether activity of the asset is allowed in the industrial network. An asset can have one of the following statuses:
  - *Authorized*. This status is assigned to an asset for which activity is allowed in the industrial network.
  - *Unauthorized*. This status is assigned to an asset for which activity is not allowed in the industrial network.
  - *Archived*. This status is assigned to an asset if it is no longer being used or must not be used in the industrial network, or if the asset has shown no activity and the asset information has not changed in a long time (30 days or more).
- **Address information** – MAC- and/or IP addresses of the asset. If an asset has multiple network interfaces, you can specify the MAC- and/or IP addresses for the network interfaces of the asset. Up to 64 network interfaces can be assigned for an asset.
- **Category** – name of the category that determines the functional purpose of the asset. Kaspersky Industrial CyberSecurity for Networks supports the following categories of assets:
  - **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.
    - **Other** – devices that do not fall into the categories described above.
- **Group** – name of the group containing the asset in the asset group tree (contains the name of the group and the names of all its parent groups).
- **Security state** – indicator of whether there are events associated with the asset. Depending on the severity levels of events, the following states are available:
    - **Critical events**. There are unprocessed events with the *Critical* severity level.
    - **Warnings**. There are unprocessed events with the *Warning* severity level but there are no unprocessed events with the *Critical* severity level.
    - **OK**. There are no unprocessed events or there are only events with the *Informational* severity level.
- **Last seen** – date and time when the last activity of the asset was registered.
- **Last modified** – date and time when information about the asset was last modified.
- **Creation date** – date and time when the asset was added to the assets table.
- **OS** – name of the operating system installed on the asset.
- **Vendor** – name of the vendor.
- **Model** – information about the model.
- **Network name** – name used to represent the asset in the network.
- **Labels** – list of labels assigned to an asset.

Viewing the assets table

The assets table is displayed in the **Assets** section of the application web interface. The assets table presents the main information about devices that are known to the application.

When viewing the assets table, you can use the following functions:

- Configure the display and order of columns in the assets table

    To configure the list of columns displayed in the table:

    1. In the **Assets** section of the application web interface, click the **Customize table** button.

       You will see a window for configuring the display of the assets table.
    2. Select the check boxes opposite the settings that you want to view in the table. You must select at least one setting.
    3. 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 assets table in the order you specified.

- Filtering based on table columns

*To filter assets based on the **Status**, **Category** or **Security state** column:*

1. In the **Assets** section, click the filtering icon in the relevant column of the table.

   When filtering by asset security states, you can also use the corresponding buttons in the toolbar.

   The filtering window opens.

2. Select the check boxes opposite the values by which you want to filter events. You can clear or remove all check boxes by clicking the link that is displayed in the upper part of the filter window.

3. Click **OK**.

*To filter assets by the **Asset ID**, **OS**, **Vendor**, **Model** or **Network name** column:*

1. In the **Assets** section, click the filtering icon in the relevant column of the table.

   The filtering window opens.

2. In the **Including** and **Excluding** fields, enter the values for assets that you want to include into the filter and/or exclude from the filter.

3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window of the selected column click the **Add condition** button and enter the condition in the opened field.

4. If you want to delete one of the created filter conditions, in the filter window of the selected column click the 🗑 icon.

5. Click **OK**.

*To filter assets by the **Address information** column:*

1. In the **Assets** section, click the filtering icon in the **Address information** column.

   The filtering window opens.

2. In the **Including** and **Excluding** fields, in the drop-down lists select the types of addresses for assets that you want to include into the filter and/or exclude from the filter. You can select the following types of addresses:

   - **IP address**
   - **MAC address**
   - **Complex** – if you want to specify multiple addresses of different types combined by the logical operator AND. To add different types of addresses, use the **Add condition (AND)** button.

3. If you want to apply multiple filter conditions by address type combined with the logical operator OR, in the filter window click the **Add condition (OR)** button and select the relevant types of addresses.

4. If you want to delete one of the created filter conditions, in the filter window click the 🗑 icon located on the right of the field containing the drop-down list.

5. Click **OK**.

*To filter assets by the **Group** column:*

1. In the **Assets** section, click the filtering icon in the **Group** column.

   The filtering window opens.

2. Click the icon in the right part of the field for indicating the group.

   The **Select group in tree** window appears.

3. In the asset group tree, select the relevant group and click the **Select** button.

   The path to the selected group will appear in the field in the filter window.

4. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window click the **Add condition** button and specify a different group in the opened field.

5. If you want to delete one of the created filter conditions, in the filter window click the 🗑 icon.

6. Click **OK**.

*To filter assets by the **Last seen**, **Last modified** or **Creation date** column:*

1. In the **Assets** section, click the filtering icon in the relevant column of the table.

   The calendar opens.

2. In the calendar, specify the date and time 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-YY hh:mm:ss.

3. Click **OK**.

To filter assets by the ***Labels*** *column:*

1. In the **Assets** section, click the filtering icon in the **Labels** column.

   The filtering window opens.

2. Enter one or multiple labels combined with the logical operator AND.

3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window click the **Add condition (OR)** button and enter the relevant labels (multiple labels in this condition will also be combined by the logical operator AND).

4. If you want to delete unnecessary labels in the filter window, you can do the following:

   - Use the ✕ icon next to the names of labels to delete the unnecessary labels.

   - Delete one of the created filter conditions by using the 🗑 icon located on the right of the field.

5. Click **OK**.

- Search assets

To find the relevant assets:

In the **Assets** section, enter your search query into the **Search assets** field. The search is initiated as you enter characters.

The assets table will display the assets that meet the search criteria.

A search is performed in all columns except the following columns: **Asset IDs**, **Status**, **Category**, **Security state**, **Last seen**, **Last modified**, and **Creation date**. The search is also performed in the values of custom fields for assets.

- Resetting the defined filter and search settings

To reset the defined filter and search settings in the assets table:

In the toolbar in the **Assets** section, click the **Clear filter** button (this button is displayed if search or filter settings are defined).

- Sorting assets

To sort assets:

1. In the **Assets** section, click the header of the column by which you want to sort.

2. When sorting assets by the **Address information** column, in the drop-down list of the column header select the setting by which you want to sort assets.

   Depending on the values selected for display in the **Address information** column, you can select one of the following options:

   - **IP address**

   - **MAC address**

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.

- Updating the assets table

Asset information could be changed on the Server while you are viewing the assets table (for example, it could be changed by another user who is connected to the Server).

To keep the assets table up to date, you can enable automatic update of the table.

To enable or disable automatic update of the assets table:

In the toolbar in the **Assets** section, use the **Autoupdate** toggle switch.

Selecting assets in the assets table

In the assets table, you can select assets to view their information and manage these assets. When assets are selected, the details area appears in the right part of the web interface window.

To select the relevant assets in the table, perform one of the following actions:

- If you want to select one asset, select the check box next to the asset or use your mouse to select the asset.
- If you want to select multiple assets, select the check boxes next to the relevant assets or select them by holding down the **CTRL** or **SHIFT** key.
- If you want to select all assets that satisfy the current filter and search settings, perform one of the following actions:
  - Select any asset 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.

When more than one asset is selected, the details area shows the quantitative distribution of the selected assets by category. If there are assets with various categories among the selected assets, you can exclude assets from one of the categories. To do so, you need to clear the check box next to the name of this category.

The title of the left-most column of the table shows the asset selection check box. Depending on the number of selected assets, the check box can have one of the following states:

- □ – all assets that satisfy the current filter and search settings were not selected in the table. However, one asset or multiple assets may be selected in the table by using the check boxes next to the assets or by using the **CTRL** or **SHIFT** key.
- ☑ – all assets that satisfy the current filter and search settings were selected in the table.
- ▣ – all assets that satisfy the current filter and search settings were selected in the table, but then the check boxes for some of the assets were cleared. This state is also retained if the check boxes were cleared for all assets selected in this way (due to the fact that the number of selected assets may change).

If all assets that satisfy the filter and search settings are selected, the number of selected assets may be automatically changed. For example, the composition of assets in the table may be changed by an application user in a different connection session or when assets are automatically added. It is recommended to configure the filter and search settings in such a way that ensures that only the relevant assets end up in the selection (for example, you can filter assets by their IDs before selecting all assets).

Automatically adding and updating assets

The application can automatically add assets to the table and update information about assets. To automatically add and update assets in Kaspersky Industrial CyberSecurity for Networks, you must enable the following asset management methods:

- Asset activity detection. When using this method, the application adds newly detected assets to the table based on the obtained MAC- and/or IP addresses of the assets. If the application detects activity of an already known asset, it may change its status depending on the current asset management mode.
- Asset Information Detection. When using this method, the application updates information about known assets based on data received from traffic.

When assets are added automatically, a name is defined for each new asset based on the following template: **Asset <value of the internal asset counter>**. The value of the internal counter in the asset name may differ from the asset ID that is displayed in the **Asset ID** column. If use of the asset information detection method is enabled, the application may update the name of an asset when it receives information about the asset.

When an asset name is updated, the application replaces the current asset name with the obtained name of the device model or its network name (the name used to represent it in the network). The network name of the asset takes priority during an update.

To update the asset name according to changes in the model name and/or in the network name, you must enable automatic updates of this information in the asset settings.

About the asset group tree

The asset group tree is intended for arranging assets according to their purpose, location, or any other attribute. For example, you can arrange assets according to groups that correspond to the location of assets within the industrial structure of the facility.

The asset group tree supports up to six nesting levels. You can add assets to groups at any level of the hierarchy. However, each asset can be added to only one of the groups in the tree.

The tree also has a limit of no more than 1000 groups.

You can specify groups for assets when manually adding an asset, when editing asset information, or when selecting multiple assets in the table. If an asset was not added to any of the groups, this asset is assigned to the top level of the hierarchy within the tree. By default, assets that are automatically added to the table are not put into groups.

You can find out which assets belong to groups when viewing the assets table. Paths to groups are indicated in the **Group** column.

Creating an asset group tree

You can create an asset group tree when working with the assets table or network map. The tree can be created in the **Create group tree** or **Select group in tree** window.

Only users with the Administrator role can create an asset group tree.

*To open the **Create group tree** window:*

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Assets** section or in the **Network map** section, click the **Configure groups** button.

Any changes made in the **Create group tree** window are immediately applied.

To select a group, the **Select group in tree** window opens when adding assets to groups or when filtering by the **Group** column. In this window, you can also access the functions for creating the asset group tree.

To create the asset group tree, you can use the following functions:

- Add group

  To add a group to the asset group tree:

  1. In the **Create group tree** or **Select group in tree** window, select the parent group or the group next to the location where you want to add a new group.
     If the tree is empty or you want to add a group on the top level of the hierarchy, skip this step and proceed to the next one.
  2. Depending on where you want to add the new group, do the following:
     - If you want to add a child group to the currently selected group, click the **Add** button or press the **`INSERT`** key.
     - If you want to add a group at the same level as the currently selected group, press **`ENTER`**.
     - If no group is selected in the tree and you want to add a group at the top level of the hierarchy, click the **Add** button or press either the **`INSERT`** or **`ENTER`** key.
  3. 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).
  4. Click the ✓ icon on the right of the entry field.

- Rename group

  To rename a group in the asset group tree:

  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 assets that are added to this group or to its child groups.

- Delete group

When a group is deleted, the assets that were added to this group or its child groups are not deleted. Instead, these assets are moved to the top level of the hierarchy within the asset tree (and information about their inclusion in the group is deleted from information regarding these assets).

To delete a group from the asset 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.
   A window with a confirmation prompt opens.
3. In the prompt window, confirm deletion of the group.

The selected group and its child groups will be removed from the tree.

- Move group

To move a group within the asset group tree:

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

To find relevant groups in the asset group tree:

In the **Create group tree** or **Select group in tree** window, enter your search query into the **Search groups** field. The search is initiated as you enter characters.

The asset group tree will display the groups that meet the search criteria. For groups that are child groups, their parent groups are also displayed.

- Update the tree

The composition of groups in the asset 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.

To update the asset group tree:

In the **Create group tree** or **Select group in tree** window, click the 🔄 icon.

Manually adding assets

You can manually add a new device to the assets table. For an added asset, you must specify a unique MAC address and/or IP address.

Only users with the Administrator role can manually add assets.

You can add assets in the following ways:

- Adding an asset when working with the assets table

To manually add an asset when working with the assets table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Assets** section, click the **Add asset** button.

   The details area appears in the right part of the web interface window.
3. On the **Addresses** tab in the details area, specify unique MAC- and/or IP addresses for the asset.
4. You can specify multiple IP addresses for the same network interface of the asset. 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.
5. If the asset has multiple network interfaces, generate a list of network interfaces of the asset 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 asset.
   - If you want to delete a network interface, click the **Delete interface** button located on the right of the name of the network interface of the asset (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.
6. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the asset information.
7. On the **Addresses** and **Settings** tabs in the details area, enable or disable automatic updates for the relevant information about the asset. To do so, use the **Autoupdate** toggle switches located above the fields that have automatic update capability.
8. On the **Custom fields** tab in the details area, create a list of custom fields if necessary.
9. Click **Save**.

   This button is unavailable if not all required information is specified in the asset settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

The assets table will show the new device with the *Authorized* status.

- Adding an asset based on a node on the network map

When working with the network map, you can add a new asset to the assets table using a node representing a device that is unknown to the application.

To add a node of an unknown device to the assets table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Assets** section and go to the **Network map** tab.
3. Select the relevant node representing the device that is unknown to the application.

   The details area appears in the right part of the web interface window.
4. Click the **Add to the Assets table** button.

   The details area will show the tabs for configuring the settings of the new asset.
5. Configure the settings of the new asset 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 an asset when working with the assets table.
6. Click **Save**.

The assets 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 an asset on the network map.

Merging assets

If one asset is represented by multiple assets in the table for some reason, these assets can be merged into one asset. Assets can be merged automatically when the asset activity detection method is enabled in learning mode. You can also manually merge assets.

> Assets are automatically merged if the application identifies a connection between the MAC address of one asset and the IP address of a different asset. If conflicts arise between defined values in asset information, the merged asset will retain the values that were defined for the asset with the IP address. For this reason, prior to enabling learning mode (and while working in this mode), it is not recommended to change information about assets for which only a MAC address is defined if they could be automatically merged with assets that have defined IP addresses.

When nodes are merged, the total number of network interfaces of the new asset must be no more than 64.

Only a user with the Administrator role can manually merge assets.

You can merge assets in the following ways:

- Merging assets when working with the assets table ?

  To manually merge multiple assets when working with the assets table:

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
  2. Select the **Assets** section.
  3. In the assets table, select the assets that you want to merge.

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

     The details area will show the tabs for configuring the settings of the new asset.
  5. Check the settings of the new asset and edit them if necessary:
     - On the **Addresses** tab in the details area, the MAC- and IP addresses of the selected assets are distributed among individual network interfaces. If necessary, change the values of addresses and the names of network interfaces.
     - On the **Settings** tab in the details area, all fields containing conflicting values in the selected assets are marked by messages regarding the conflicting values. The conflicting values are merged into one value in text fields.
     - On the **Custom fields** tab in the details area, the list contains all custom fields of the selected assets.
  6. Click the **Merge** button.

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

  The assets table will show the new device with the *Authorized* status.

- Merging assets when working with the network map ?

When working with the network map, you can merge multiple nodes on the network map into one new asset for the assets table.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

WAN nodes cannot be merged.

To merge assets represented by nodes on the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select multiple objects representing nodes and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.
3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
4. Click the **Merge assets** button.

   The details area will show the tabs for configuring the settings of the new asset.
5. Check the settings of the new asset and edit them if necessary:

   - On the **Addresses** tab in the details area, the MAC- and IP addresses of the selected assets are distributed among individual network interfaces. If necessary, change the values of addresses and the names of network interfaces.
   - On the **Settings** tab in the details area, all fields containing conflicting values in the selected assets are marked by messages regarding the conflicting values. The conflicting values are merged into one value in text fields.
   - On the **Custom fields** tab in the details area, the list contains all custom fields of the selected assets.
6. Click the **Merge** button.

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

The assets 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 assets

You can delete one or multiple assets from the assets table.

Only a user with the Administrator role can delete assets.

Information about deleted assets is not saved in the application. If deleted assets start displaying activity in the industrial network again, the application will add them to the assets table as new assets (with the *Authorized* or *Unauthorized* status depending on the current asset management mode).

You can delete assets in the following ways:

- Deleting assets when working with the assets table ?

To delete assets when working with the assets table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Assets** section.
3. In the assets table, select the assets that you want to delete.

   The details area appears in the right part of the web interface window.
4. Click **Delete asset** (if one asset is selected) or **Delete assets** (if multiple assets are selected).

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

- Deleting assets when working with the network map ?

When working with the network map, you can remove assets from the assets table by using the nodes representing those assets on the network map.

To remove an asset when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select one or multiple nodes representing assets.

   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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes while also indicating how many of the assets belong to each category.
3. If there are assets with various categories among the selected nodes, you can exclude assets from one of the categories. To do so, clear the check box next to the name of this category. The category name will disappear from the list.
4. Click the **Delete asset** button (if one node is selected) or **Delete assets** (if multiple nodes are selected).

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

Automatically changing the statuses of assets

When monitoring the activity of assets in the industrial network, the application automatically assigns the appropriate statuses to detected devices based on the obtained MAC- and/or IP addresses of devices.

In learning mode, the *Authorized* status is assigned to all detected devices.

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 not in the assets table when it is detected, the *Unauthorized* status is assigned to this device.
- If the device is in the assets table and has the *Authorized* or *Unauthorized* status, the status is not changed.
- If the device is in the assets table with the *Archived* status, the *Unauthorized* status is assigned to this device.

If an asset with the *Authorized* status has not shown any activity and information about this asset has not been changed in a long time (30 days or more), the *Archived* status is assigned to this asset.

When assets with the *Unauthorized* status appear in the assets table, you need to determine whether all of these assets are required for industrial process support. After making this determination, it is recommended to manually assign one of the following statuses to each asset:

- *Authorized* – if the asset is required for industrial process support.
- *Archived* – if the asset should not be used in the industrial network.

> Instead of assigning the *Archived* status, you can delete the asset. However, all information specified for the asset will also be deleted. If a deleted asset is detected again, the application will provide only the information that has been received since the asset was re-added to the assets table (the date and time of the first detection of the asset is also updated).

Manually changing the statuses of assets

Only a user with the Administrator role can change the statuses of assets.

You can change the status for one selected asset or for multiple selected assets simultaneously. If one asset with the *Archived* status is selected, the status of this asset can be changed only when information about the asset is changed. If multiple assets are selected, you can assign any status to these assets, regardless of their current status.

> The application automatically changes the status of an *Archived* asset if it displays activity. Depending on the current asset management mode, the application assigns either the *Authorized* or *Unauthorized* status to the detected asset.

You can change the statuses of assets in the following ways:

- Changing the statuses of assets when working with the assets table ?

  To change the status of assets when working with the table:

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
  2. Select the **Assets** section.
  3. In the assets table, select the assets whose status you want to change.

     The details area appears in the right part of the web interface window.
  4. Depending on the current status and number of selected assets, perform one of the following actions:
     - If multiple assets are selected, click the button with the name of the relevant status.
     - If one asset with the *Authorized* or *Unauthorized* status is selected, click the button containing the name of the necessary status (a button containing the name of the current status is not displayed).

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

- Changing the statuses of assets when working with the network map ?

When working with the network map, you can change the statuses of known assets represented by nodes on the network map.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To change the status of assets when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select one or multiple objects representing nodes of assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.
3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
4. Depending on the current status and number of selected nodes, perform one of the following actions:

   - If multiple nodes representing known assets are selected, click the button with the name of the relevant status.
   - If one node representing an asset with the *Authorized* or *Unauthorized* status is selected and you want to assign a different status to this asset, click the button containing the name of the necessary status (a button containing the name of the current status is not displayed).

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

Viewing asset information

Detailed information about an asset includes information from the assets table, and the following fields:

- **Router** – indicator of a routing device.
- **Additional information** – additional information about an asset specified by an application user.
- **Custom fields** – set of user-defined information that is absent from the standard set of information. Up to 16 custom fields may be specified for an asset.

To view asset information:

In the **Assets** section, select the relevant asset.

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.

Managing the arrangement of assets in the group tree

You can manage the arrangement of assets in the group tree by adding assets to the relevant groups or excluding assets from groups.

Until an asset is added to a specific group, information about this asset does not contain any information about the specific location of the asset. This asset is assigned to the top level of the hierarchy within the group tree. After an asset is added to a group, the application saves the location of this asset as the full path to the group in the group tree.

Only users with the Administrator role can manage the location of assets within the group tree.

To manage the arrangement of assets in the group tree, you can use the following functions:

- Add one asset to a group

  To add an asset to a group:

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
  2. Select the asset in the **Assets** section or in the **Network map** section.

     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 asset 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 asset settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

- Add multiple assets to a group

You can add multiple assets to a group when working with the assets table.

When working with the network map, you can also add multiple known assets represented by nodes on the network map to a group. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To add multiple assets to a group when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Assets** section.
3. In the assets table, select the assets that you want to add to a group.

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

To add multiple assets to a group when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select the relevant nodes of assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.
3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
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 asset 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 selected nodes representing known assets will be displayed within the selected group.

- Remove one asset from a group ?

To remove an asset from a group:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the asset in the **Assets** section or in the **Network map** section.

   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 **Clear** link above the field (the link is displayed if a group is defined).
6. Click **Save**.

   This button is unavailable if not all required information is specified in the asset 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 asset, the **Group** parameter is cleared and the asset will be assigned to the top level of the hierarchy within the group tree.

- Remove multiple assets from groups

You can remove multiple assets from groups when working with the assets table. The assets selected for removal from groups may be part of the same group or in different groups.

When working with the network map, you can also remove multiple known assets represented by nodes on the network map from groups. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To remove multiple assets from groups when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Assets** section.
3. In the assets table, select the assets that you want to remove from groups.

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

For all selected assets, the **Group** parameter is cleared and these assets will be assigned to the top level of the hierarchy within the group tree.

To remove multiple assets from groups when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select the nodes in expanded groups and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.
3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
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 assets from groups.

For all selected assets, the **Group** parameter is cleared and these assets will be displayed outside of groups.

Adding and removing labels for assets

You can assign any user-defined labels to assets.

An *asset label* contains a text description that helps you quickly find or filter assets in the table. Any convenient text descriptions can be saved as labels. You can assign up to 16 labels for an asset. Each asset can have its own set of labels.

Lists of asset labels are displayed in the assets 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 assets.

Labels can be added or removed in the following ways:

- Adding labels for one asset ?

To add labels for an asset:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the asset in the **Assets** section or in the **Network map** section.

   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 asset 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 asset settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

- Adding labels for multiple assets ?

You can add labels for multiple assets when working with the assets table.

When working with the network map, you can also add labels for known assets that are represented by nodes on the network map. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To add labels for multiple assets when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Assets** section.
3. In the assets table, select the assets for which you want to add labels.

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

   The **Add labels** window opens.
5. 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 asset labels (not case-sensitive)
   - Contains from 1 to 255 characters
6. 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.
7. If you want to clear the current lists of labels for selected assets and provide only new labels for these assets, select the **Delete existing** check box.

   > If the **Delete existing** check box is cleared, the current list of labels will remain on each asset. The new labels will be added to the lists of labels on all selected assets. In this case, the total number of labels for some of the selected assets may exceed the limit (up to 16 labels for each asset). The application checks this limit before adding new labels.
8. 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 assets when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, select the relevant nodes of assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.
3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
4. Click the **Add labels** button.

   The **Add labels** window opens.
5. 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 asset labels (not case-sensitive)
   - Contains from 1 to 255 characters
6. 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.

7. If you want to clear the current lists of labels for selected assets and provide only new labels for these assets, select the **Delete existing** check box.

   > If the **Delete existing** check box is cleared, the current list of labels will remain on each asset. The new labels will be added to the lists of labels on all selected assets. In this case, the total number of labels for some of the selected assets may exceed the limit (up to 16 labels for each asset). The application checks this limit before adding new labels.

8. 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 asset

To clear the list of asset labels:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the asset in the **Assets** section or in the **Network map** section.

   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.
   - Click the **Clear** link above the list of labels if you want to remove all labels.

5. Click **Save**.

   This button is unavailable if not all required information is specified in the asset 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 assets

You can clear the lists of labels for multiple assets when working with the assets table.

When working with the network map, you can also clear the lists of labels for known assets that are represented by nodes on the network map. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To clear the lists of labels for multiple assets when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the **Assets** section.

3. In the assets table, select the assets for which you want to clear the lists of labels.

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

4. Click the **Add labels** button.

   The **Add labels** window opens.

5. Select the **Delete existing** check box.

6. Click **OK**.

To clear the lists of labels for multiple assets when working with the network map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Network map** section, select the relevant nodes of assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.

3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.

4. Click the **Add labels** button.

   The **Add labels** window opens.

5. Select the **Delete existing** check box.

6. Click **OK**.

Editing asset information

Only users with the Administrator role can change asset information.

To manually edit asset information:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Assets** section, select the relevant asset.

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

3. Click the **Edit** button.

   The details area will show the tabs for viewing and editing asset information: **Addresses**, **Settings** and **Custom fields**.

4. On the **Addresses** tab in the details area, specify the MAC- and/or IP addresses of the asset.

   You can specify multiple IP addresses for the same network interface of the asset. 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.

5. If the asset has multiple network interfaces, generate a list of network interfaces of the asset and specify the corresponding MAC- and/or IP addresses for them.

   To generate a list of network interfaces of an asset, 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 asset.
   - If you want to delete a network interface, click the **Delete interface** button located on the right of the name of the network interface of the asset (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.

6. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the asset information.

   > Also on the **Settings** tab, you can change the status of an asset (for example, assign any other status to an asset with the *Archived* status).

7. On the **Addresses** and **Settings** tabs in the details area, enable or disable automatic updates for the relevant information about the asset. To do so, use the **Autoupdate** toggle switches located above the fields that have automatic update capability.

8. On the **Custom fields** tab in the details area, create a list of custom fields and their values if necessary.

9. Click **Save**.

   This button is unavailable if not all required information is specified in the asset settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the ⚠ icon.

Adding, editing and deleting custom fields for an asset

You can add, edit and delete custom fields containing information about assets. Custom fields are displayed in the details area when an asset is selected.

For custom fields, the following limitations apply:

- The number of custom fields for one asset 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 1024.

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 a web browser using the account credentials of a user with the Administrator role.
2. In the **Assets** section, select the relevant asset.

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

   The details area will show the tabs for viewing and editing asset information: **Addresses**, **Settings** 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**.

Viewing events associated with assets

You can view events associated with assets. Events are loaded by automatically applying a filter based on the IDs of assets using the values of the MAC- and IP addresses specified for the assets.

In the events table, the application shows events whose **Source** or **Destination** columns contain the MAC- or IP addresses of selected assets.

Events can be loaded if no more than 200 assets are selected.

To view events associated with assets:

1. Select the **Assets** section.
2. In the assets table, select the assets for which you want to view events.

   The details area appears in the right part of the web interface window.
3. Depending on which events you want to load, click one of the following buttons (the buttons are unavailable if more than 200 assets are selected):
   - **Show events** – if you want to view events with any status.
   - **Show unprocessed events** – if you want to view events with the *New* or *In progress* status.

The **Events** section opens. The events table will apply a filter based on the IDs of assets. The list of asset IDs defined for event filtering is displayed in the **Asset IDs** field in the toolbar. If you loaded events by using the **Show unprocessed events** button, events will also be filtered by the **Status** column.

Network Control

To control an industrial network using Kaspersky Industrial CyberSecurity for Networks, you can configure monitoring of the communications between devices in the industrial network.

The application monitors communications between industrial network devices based on Network Control rules. A *Network Control rule* describes the authorized communications for devices.

A Network Control rule can apply 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.

Generally, a Network Control rule contains the following information about communications:

- Sides participating in network communications.
- Allowed protocol or system commands.

Network Control rules may be active or inactive.

By default, a rule is active 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 active network control rules.

Inactive rules are intended for describing unwanted network communications. . In Network Control learning mode, inactive rules prevent automatic creation of new active rules for detected network interactions that are described in inactive rules. In Network Control monitoring mode, inactive rules are not taken into account.

The application processes network control rules based on Network Integrity Control and Command Control technology if the use of these technologies is enabled.

The following methods are provided for creating a list of Network Control rules:

- Automatic generation of rules in learning mode.
- Manual creation of rules.

The list of Network Control rules is stored on the Server and is independent of the security policy loaded in the Console or applied on the Server.

You can configure network control rules in the **Network Control** section of the Kaspersky Industrial CyberSecurity for Networks web interface.

You can configure the settings for registration of Network Control events in the Application Console on the **Configure events** tab. Events registered based on Network Integrity Control and Command Control technologies are categorized as system events.

You can view Network Control events in the table of registered events. Events registered based on Network Integrity Control technology have the *Warning* severity level. Events registered based on Command Control technology are assigned a severity that depends on the severity level defined for the detected system command.

Network Control learning mode

In Network Control learning mode, Kaspersky Industrial CyberSecurity for Networks performs the following actions:

- If use of Network Integrity Control technology is enabled, the application generates rules based on this technology. When the application detects network communications matching inactive rules, it registers events based on Network Integrity Control technology. The event is 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 satisfy inactive 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 Network Control rules, the application adds new rules from analysis of network communications 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 communications detected during traffic analysis are checked for compliance with current Network Control rules. If a detected interaction does not match any rule, the application creates a new Network Control rule. In this case, an interaction detection event is not registered. When a new rule is created, the application makes it active and adds settings values based on the received data about the network interaction.

If the detected interaction only matches an inactive rule, the application registers an event based on the technology corresponding to this rule. A new active rule is not created.

During the learning process, the application can optimize the list of Network 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 active.
- 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 Network Control rule was created after a system command was detected during an interaction between two devices. Then another system command was detected during an interaction between these 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.

The application periodically optimizes the list of Network Control rules while operating in learning mode. 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 rule list is 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, we recommend that you not make any changes to the rules generated in learning mode.

Network Control learning mode must be enabled for enough time to receive all the necessary data 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.

Network Control monitoring mode

In Network Control monitoring mode, Kaspersky Industrial CyberSecurity for Networks performs the following actions:

- 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 active rules, it registers unauthorized communication detection events based on Network Integrity Control technology. The event is 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 active 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 list of Network Control rules must have rules for this system command and for the network packet that transmits it.

Selecting the applied technologies and changing the Network Control mode

Only users with the Administrator role can manage Network Control modes and technologies.

To enable or disable the use of Network Control technologies:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Technologies** tab.
3. Enable or disable the use of Network Control technologies by using the following toggle switches:
   - **Network Integrity Control**
   - **Command Control**
4. After a technology is enabled or disabled, wait for the toggle switch to change to the necessary position (*Enabled* or *Disabled*).

The process may take some time, during which the toggle switch will be unavailable. Wait for the technology to be enabled or disabled.

5. For each enabled technology, select the necessary Network Control mode. To do so, in the drop-down list on the right of the technology name, select one of the following values:
   - **Learning** – to apply the technology in learning mode.
   - **Monitoring** – to apply the technology in monitoring mode.
6. After the mode is selected, wait for the name of this mode to appear in the field of the drop-down list.
7. This process may take some time, during which the drop-down list displays the *Changing* status. Wait for the selected mode to be enabled.

Automatic generation of Network Control rules in learning mode

In learning mode, Kaspersky Industrial CyberSecurity for Networks automatically generates Network Control rules by analyzing the network interactions between devices in the industrial network. The application creates a new rule if the detected network interaction does not match any rule in the list of Network Control rules.

In learning mode, the application can automatically create Network Control rules that allow transmission of system commands for Kaspersky Industrial CyberSecurity for Nodes. These rules are needed for integration of Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes within the integrated solution Kaspersky Industrial CyberSecurity. 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 installed in this same industrial network. For detailed information on enabling components of Kaspersky Industrial CyberSecurity for Nodes, please refer to the *Administrator's Guide for Kaspersky Industrial CyberSecurity for Nodes*.

Viewing the table of Network Control rules

The table of Network Control rules is displayed in the **Network Control** section of the application web interface.

When viewing the table of Network Control rules, you can use the following functions:

- Configure the display and order of columns in the rules table

To configure the list of columns displayed in the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser and select the **Network Control** section.
2. Click the **Customize table** button.

   You will see a window for configuring the display of the rules table.
3. Select the check boxes opposite the settings that you want to view in the table. You must select at least one setting.

   The following settings are available for selection:

   - **Rule ID**

     Unique ID of the rule.
   - **State** (the ◐ icon)

     The current state of the rule (*Active* or *Inactive*).
   - **Technology**

     Technology associated with the rule.
   - **Protocols/Commands**

     For rules related to Network Integrity Control technology – the set of utilized protocols. For rules related to Command Control technology – the protocol and system commands. The protocols that are determined by the application based on the contents of network packets are italicized.
   - **Side 1**

     Address information of one of the sides of network interaction:

     - **MAC address**
     - **IP address**
     - **Port number**
   - **Side 2**

     Address information of the other side of network interaction:

     - **MAC address**
     - **IP address**
     - **Port number**
   - **Comment**

     Additional information about the rule.
   - **Creation date**

     The date and time when the rule was created.
   - **Modification date**

     The date and time when the rule was last modified.
   - **Origin**

     Information about the origin of the rule.
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.

   For the **Side 1** and **Side 2** columns, you can also change the order in which the address information is displayed for the sides of network interaction. To do so, select the value that you want to move 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 network control rules table in the order you specified.

- Filtering based on table columns

*To filter rules by the **Rule ID** column:*

1. In the **Network Control** section, click the filtering icon in the **Rule ID** column.

   The filtering window opens.

2. In the **Including** and **Excluding** fields, enter the values for rules that you want to include into the filter and/or exclude from the filter.

3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window of the column click the **Add condition** button and enter the condition in the opened field.

4. If you want to delete one of the created filter conditions, in the filter window of the column click the 🗑 icon.

5. Click **OK**.

*To filter rules based on the **State**, **Technology** or **Origin** column:*

1. In the **Network Control** section, click the filtering icon in the relevant column.

   When filtering based on the states, technologies, or origins of Network Control rules, you can also use the corresponding buttons in the toolbar.

   The filtering window opens.

2. Select the check boxes opposite the values by which you want to filter events.

3. Click **OK**.

*To filter rules by the **Protocols/Commands** column:*

1. In the **Network Control** section, click the filtering icon in the **Protocols/Commands** column.

   > Filtering by the **Protocols/Commands** column is applied only for protocols. To filter Network Control rules based on the names of system commands, you can use the rule search function.

   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**.

*To filter rules based on the **Side 1** and **Side 2** columns:*

1. In the **Network Control** section, open the **Address information** drop-down list.

   The filtering window opens.

2. Specify the necessary values in the following fields:

   - **MAC address**
   - **IP address**
   - **Port number**

3. Click **OK**.

*To filter rules based on the **Creation date** or **Modification date** column:*

1. In the **Network Control** section, click the filtering icon in the relevant column.

   The calendar opens.

2. In the calendar, specify the date and time 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-YY hh:mm:ss.

3. Click **OK**.

- Rule search

To find the relevant rules:

In the **Network Control** section, enter your search query into the **Rule search** field. The search is initiated as you enter characters.

The Network Control rules table displays the rules that meet the search criteria.

A search is performed in all columns except the **State**, **Technology**, **Creation date**, **Modification date** and **Origin** columns.

- Resetting the defined filter and search settings

To reset the defined filter and search settings in the network control rules table:

In the toolbar in the **Network Control** section, click the **Clear filter** button (this button is displayed if search or filter settings are defined).

- Sorting rules

To sort network control rules:

1. In the **Network Control** section, click the header of the column by which you want to sort.

   You can sort the table of Network Control rules based on the values of any column except the **Comment** column.

2. When sorting rules by the **Protocols/Commands**, **Side 1** or **Side 2** column, in the drop-down list of the column header select the setting by which you want to sort rules:

   - In the **Protocols/Commands** column, select the sorting settings: by protocol or by system command.
   - Depending on the values selected for display in the **Side 1** or **Side 2** columns, select the sorting settings: by MAC address, by IP address, or by port number.

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.

- Updating the rules table

Network control rules could be changed on the Server while you are viewing the rules table. For example, the Network Control rules table becomes outdated if an application user in a different connection session changes rules or if the application optimizes the list of rules in learning mode.

To keep the table of network control rules up to date, you can enable automatic update of rules or manually update the table. During updates, all rules are reloaded from the Server.

To enable or disable automatic update of the table of Network Control rules:

In the **Network Control** section, use the **Autoupdate** toggle switch.

When automatic update is enabled, the table of network control rules is updated every five seconds.

To manually update the table of Network Control rules:

1. Disable automatic update if this function is enabled. To do so, in the **Network Control** section, set the **Autoupdate** toggle switch to *Disabled*.

2. Click the **Refresh** button (this button is displayed on the right of the **Autoupdate** toggle switch if the toggle switch is disabled).

   The rules table is reloaded from the Server.

Selecting Network Control rules

In the table of Network Control rules, you can select rules to view their information and manage these rules. When rules are selected, the details area appears in the right part of the web interface window.

To select the relevant Network Control rules, perform one of the following actions:

- If you want to select one rule, select the check box next to the rule or use your mouse to select the rule.
- If you want to select multiple rules, select the check boxes next to the relevant rules or select the rules while holding down the **CTRL** or **SHIFT** key. When multiple rules are selected, the application checks the state of the selected rules and determines whether there are active and inactive rules among the selected rules.
- If you want to select all rules that satisfy the current filter and search settings, perform one of the following actions:
  - Select any rule 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.

When multiple rules are selected, the details area shows the total number of selected rules. If you selected all rules that satisfy the current filter and search settings, one of the following values appears in the details area:

- The precise number is displayed if you selected 1000 rules or less. In this case, the application checks the state of the selected rules just as with other methods for selecting multiple rules.
- If more than 1000 rules are selected, the number **1000+** is displayed. In this case, the application does not check the state of the selected rules.

The title of the left-most column of the table shows the rule selection check box. Depending on the number of selected rules, the check box can have one of the following states:

- □ – all rules that satisfy the current filter and search settings were not selected in the table. However, one rule or multiple rules may be selected in the table by using the check boxes next to the rules or by using the **CTRL** or **SHIFT** key.
- ☑ – all rules that satisfy the current filter and search settings were selected in the table.
- ▣ – all rules that satisfy the current filter and search settings were selected in the table, but then the check boxes for some of the rules were cleared. This state is also retained if the check boxes were cleared for all rules selected in this way (due to the fact that the number of selected rules may change).

If all rules that satisfy the filter and search settings are selected, the number of selected rules may be automatically changed. For example, the composition of rules in the table may be changed by an application user in a different connection session or when the list of rules is optimized in learning mode. It is recommended to configure the filter and search settings in such a way that ensures that only the relevant rules end up in the selection (for example, you can filter rules by their IDs before selecting all rules).

Manually creating Network Control rules

The following options are provided for manually creating Network Control rules:

- Starting with empty values of settings
- Based on an existing rule

- Based on events registered for Network Integrity Control or Command Control technology

To create a rule with initially empty values of settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Network Control** section, click the **Add rule** button.

   The details area in rule editing mode will appear in the right part of the web interface window.

3. Select a technology for the rule:

   - 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.

4. 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 specify 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.

5. 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**.

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 address information for the sides of network interaction that is available for editing. Depending on the selected protocol (or set of protocols), address information may contain the following values:

   - MAC address

- IP address
- Port number

8. Click **Save**.

   The application will check the table of Network Control rules.

9. If the rules table contains an active 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.

10. If the rules table contains an active 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 list of Network Control rules.

11. If the rules table contains active 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 inactive 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.

12. If there is no active rule allowing network interaction between devices for a new rule related to Command Control technology, you will be prompted to create the corresponding rule related to 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 related to Network Integrity Control technology.

To create a new Network Control rule based on an existing rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Network Control** 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 the context menu, select **Create rule based on the selected 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 3–8 described in the procedure for creating a rule with initially empty values of settings.

To create a new network control rule based on a registered event:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

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 the network control rule. You can select an event that was registered based on *Network Integrity Control* technology or *Command Control* technology. However, the event must contain information only about one network interaction.

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

4. In the details area, click the **Create Network Control rule** button.

   In the web browser window, the **Network Control** section opens. 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 4–8 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 using the **Save** button.

Editing Network Control rule settings

You can edit the settings of an active Network Control rule. You cannot edit inactive rules.

To edit Network Control rule settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Network Control** section, select the relevant rule whose settings you want to edit.

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

3. Click the **Edit** button.

4. Change the settings as necessary. For a description of the actions necessary for configuring settings, please refer to the procedure for creating a rule with initially empty values of settings in the Manually creating Network Control rules section.

Changing the state of Network Control rules

Network Control rules may be active or inactive. By default, each rule has active state after its creation.

You can switch rules to inactive state to disable their use when Network Control is in monitoring mode.

To switch Network Control rules to inactive state:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. In the **Network Control** section, select one or multiple active rules whose state you want to change.

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

3. Depending on the number of selected rules, click the **Deactivate rule** or **Deactivate rules** button. The button is not displayed if you selected only inactive rules. If all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1000, the application does not

check the state of rules. In this case, the **Deactivate rules** button is displayed regardless of the state of the selected rules.

To switch Network Control rules to active state:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network Control** section, select one or multiple inactive rules whose state you want to change.

   The details area appears in the right part of the web interface window.
3. Depending on the number of selected rules, click the **Activate rule** or **Activate rules** button. The button is not displayed if you selected only active rules. If all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1000, the application does not check the state of rules. In this case, the **Activate rules** button is displayed regardless of the state of the selected rules.

Deleting Network Control rules

You can selectively delete one or multiple Network Control rules. Rules that are deleted are no longer applied for Network Control, whether in monitoring mode or learning mode.

To delete Network Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Network Control** section.
3. In the rules table, select the rules that you want to delete.

   The details area appears in the right part of the web interface window.
4. Depending on the number of selected rules, click the **Delete rule** or **Delete rules** 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 in active state, the application prompts you to delete the selected rules, switch them to inactive state, 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 1000.
   - If there are inactive 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 1000, the application prompts you to delete the selected rules or cancel the operation.
5. In the prompt window, confirm deletion of the rules.

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 rules and additional Intrusion Detection methods based on embedded algorithms are applied regardless of the security policy loaded in the Console or applied on the Server.

You can configure Intrusion Detection rules in the Kaspersky Industrial CyberSecurity for Networks Console on the **Intrusion detection** tab.

You can change the state of Intrusion Detection methods when connected to the Server through a web browser.

You can configure the settings for registration of Intrusion Detection events in the Application Console on the **Configure events** tab.

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.

Intrusion Detection rules are included in rule sets. A rule set includes Intrusion Detection rules grouped according to any attributes (for example, rules that contain interdependent traffic analysis conditions). The following types of rule sets may be used in the application:

- 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.
- Custom 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 custom rule sets must match the names of the files from which these rule sets were loaded (not including the file extensions).

Intrusion Detection rule sets may be active or inactive. Active state means that rules from the set are applied during traffic analysis if the rule-based Intrusion Detection method is enabled. If a rule set has been switched to inactive, the rules from this set are no longer applied.

When a rule set is loaded, the application checks the rules in the set. If errors are found when the rule set is checked (for example, duplicated rules are detected), the application displays information about the number of detected errors for this set. Rule sets with detected errors are ignored in the application (the rules from these sets are not applied, even if the sets are active).

When the conditions defined in an active Intrusion Detection rule 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 custom rule set is triggered.

The severity levels of Kaspersky Industrial CyberSecurity for Networks events correspond to the priorities in Intrusion Detection rules (see the table below).

Mapping between rule priority and event severity

Intrusion Detection rule priority	Kaspersky Industrial CyberSecurity for Networks event severity
4 or higher	Informational
2 or 3	Warning
1	Critical

Additional Intrusion Detection methods

You can apply the following additional methods for Intrusion Detection:

- Detection of signs of falsified addresses in ARP packets

  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 event is 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.

You can apply additional Intrusion Detection methods regardless of the presence and state of Intrusion Detection rules. Embedded algorithms are used for the additional scan methods.

Enabling and disabling rule-based Intrusion Detection

You can enable and disable use of the rule-based Intrusion Detection method when connected to the Server through a web browser.

Only users with the Administrator role can enable and disable the rule-based Intrusion Detection method.

To enable or disable the rule-based Intrusion Detection method:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section and go to the **Technologies** tab.

3. Use the **Rule-based Intrusion Detection** toggle switch to enable or disable rule-based Intrusion Detection.

4. After a method is enabled or disabled, wait for the toggle switch to change to the necessary position (*Enabled* or *Disabled*).

   This process takes some time. The toggle switch will be unavailable during this time.

Enabling and disabling additional Intrusion Detection methods

You can enable and disable use of additional Intrusion Detection methods when connected to the Server through a web browser.

Only users with the Administrator role can enable and disable the additional Intrusion Detection methods.

To enable or disable additional Intrusion Detection methods:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.

2. Select the **Settings** section and go to the **Technologies** tab.

3. Enable or disable the use of additional Intrusion Detection methods by using the following toggle switches:

   - **ARP spoofing detection** – enables or disables detection of signs of falsified addresses in ARP packets.

   - **TCP protocol anomaly detection** – enables or disables TCP protocol anomaly detection.

   - **IP protocol anomaly detection** – enables or disables IP protocol anomaly detection.

4. After a method is enabled or disabled, wait for the toggle switch to change to the necessary position (*Enabled* or *Disabled*).

   This process takes some time. The toggle switch will be unavailable during this time.

Viewing the table containing sets of Intrusion Detection rules

When viewing the table containing sets of Intrusion Detection rules, you can use the following functions:

- Filter the table

  To filter the table containing sets of Intrusion Detection rules:

  1. On the **Intrusion detection** tab, click the filtering icon in the column by which you want to filter.

     You can filter by any column except the **Name of rules set** column.

  2. In the drop-down list, select the setting for filtering sets of rules.

  The table containing sets of Intrusion Detection rules will display only those sets of rules that satisfy the selected filter setting.

- Search sets of rules

  To find sets of Intrusion Detection rules:

  On the **Intrusion detection** tab, enter your search query into the **Search** field. The search is initiated as you enter characters.

  The table containing sets of Intrusion Detection rules will display the rule sets that meet the search criteria.

  The search is performed based on the **Name of rules set** column.

- Sorting sets of rules

  To sort sets of Intrusion Detection rules based on the values of a column:

  1. On the **Intrusion detection** tab, click the arrow icon in the right part of the header of the column by which you want to sort.

     The table will be sorted by the selected column. The arrow icon will take the appearance corresponding to the current sort order.

  2. If you want to reverse the sorting order, click the arrow icon again.

Changing the state of sets of Intrusion Detection rules

Intrusion Detection rule sets may be active or inactive. If a set of rules has been switched to inactive state, no rules in this set are used for Intrusion Detection.

Only users with the Administrator role can change the states of sets of Intrusion Detection rules.

To change the state of sets of Intrusion Detection rules:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. Select the **Intrusion detection** tab in the Application Console window.
3. In the table containing sets of Intrusion Detection rules, select or clear the check boxes in the **Active** column for those rule sets whose state you want to change.

   The lines containing sets of rules whose state will be changed are distinguished by their color.
4. Click the **Apply** button.

Rule state will change in accordance with the boxes you check/uncheck. After switching a set of rules to inactive state, the line corresponding to the set of rules will be displayed in cursive.

Loading and replacing custom 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. 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 custom set of rules. The name of the set of rules will match the name of the file without the RULES extension.

When sets of rules are loaded from files, the current custom sets of rules 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 custom sets of Intrusion Detection rules.

To load and replace custom sets of Intrusion Detection rules:

1. Make sure that you have the permissions to read files in the folder containing the Intrusion Detection rule files that you want to use.
2. Start the Application Console and provide the account credentials of a user with the Administrator role.
3. Select the **Intrusion detection** tab in the Application Console window.
4. In the toolbar, open the **Custom rules** menu and select **Replace custom rules**.

   The **Folder containing files with Intrusion Detection rules** window opens.
5. Specify the directory with Intrusion Detection rule files.
6. Click the **Select** button.

   The table containing sets of rules displays the new custom sets of rules. For these sets of rules, the **Origin** column will show the **User** value. All sets of rules will be in active state.
7. Check for errors in the loaded sets of rules. Information about detected errors is displayed in the **Errors** column. If the set of rules contains errors, you can view detailed information about them by clicking the **Details** link.
8. If you do not want to use some of the sets of rules for Intrusion Detection, change their state.

Removing custom sets of Intrusion Detection rules

You can remove all custom sets of Intrusion Detection rules that were loaded into the application from files. You cannot selectively remove individual custom sets of rules.

When custom sets of rules are removed, the files from which those sets of rules were loaded are not deleted. The files can be used to load the rules again (for example, if you want to selectively load files).

Only users with the Administrator role can delete custom sets of Intrusion Detection rules.

To delete custom sets of Intrusion Detection rules:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. Select the **Intrusion detection** tab in the Application Console window.
3. In the toolbar, open the **Custom rules** menu and select **Delete custom rules**.

   The **Delete custom rules** menu item is available if the table has custom sets of Intrusion Detection rules.

   A window with a confirmation prompt opens.
4. Click **Yes**.

All custom 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 log entries in the database

You can change the settings for storing log entries in the database.

To change the settings for storing application entries:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Logs**.

   The **Manage logs** window opens.
3. On the **Logging settings** tab, in the **Audit**, **Event history** and **Application messages** groups of settings, configure the following settings:
   - **Maximum period for keeping log records (in days)**

     The default value of this setting is 365 days.
   - **Maximum number of log records**

     The default value of this setting is 100,000 entries. When changing the value of this setting, please note the estimated volume of disk space usage for the specified number of entries.
4. Click the **Apply** button.

Managing the settings for saving traffic in the database

The application can save traffic at the moment events are registered and store that traffic in the 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 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 database:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Logs**.

   The **Manage logs** window opens.
3. Select the **Save traffic** tab.
4. Configure the following settings for saving traffic in the database:
   - **Maximum number of saved packets**

     The default value of this setting is 100,000,000 packets.

   - **Maximum period for storing packets (in days)**

     The default value of this setting is 365 days.

   - **Maximum size of saved traffic in the database (MB)**

     The default value of this setting is 15000 MB.

5. Click the **Apply** button.

Enabling and disabling the user activity audit

You can enable or disable the user activity audit when connected to the Server through a web browser or in the Application Console.

User activity audit is enabled by default.

To enable or disable the user activity audit when connected to the Server through a web browser:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Audit** tab.
3. Use the **User activity audit** toggle switch 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.

To enable or disable the user activity audit in the Application Console:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Logs**.

   The **Manage logs** window opens.
3. On the **Logging settings** tab, perform the necessary action:
   - If you want to enable the audit, select the **Enable** check box in the **Audit** block.
   - If you want to disable the audit, clear the **Enable** check box in the **Audit** block.
4. Click the **Apply** button.

Changing the log level for processes

You can manage how data is saved in logs of the following application processes:

- ProductFacade
- ProductServer

- KisClient
- Filter
- NetworkDumper
- EntityManager
- Watchdog

For each process, you can assign one of the following log levels:

- **Critical**. Data on process failures that could have a critical impact on the application is saved in the log.
- **Error**. The log saves **Critical** level data and information about errors that occur while the process is running.
- **Warning**. The log saves **Error** level data and data requiring attention.
- **Informational**. The log saves **Warning** level data and reference information.
- **Debug**. The log saves **Informational** level data and all process data that may be required during the application debugging process (such as auxiliary messages and process performance data).

The log levels may need to be changed, for example, when contacting Technical Support.

To change the log level of a Kaspersky Industrial CyberSecurity for Networks process:

1. Start the Application Console and provide the account credentials of a user with the Administrator role.
2. In the **Settings** menu of the Application Console window, select **Server and sensors**.

   The **Settings of Server and sensors** window opens.
3. On the **Operating mode** tab, expand the list of processes of the relevant node in the **Node** column.
4. If a process whose log level you need to change is associated with a specific component (Server or sensor), expand the list of processes of that component.
5. In the drop-down list of the **Log level** column, assign the log level for the relevant process.
6. Click the **Apply** button.

Managing technologies

In the web interface of Kaspersky Industrial CyberSecurity for Networks, you can enable or disable the use of technologies, and change the operating mode of technologies. Only users with the Administrator role can manage technologies.

The following technologies and methods can be enabled and disabled:

- Network Control technologies:
  - Network Integrity Control

    - Command Control
- Asset Management methods:
    - Asset activity detection
    - Asset Information Detection
    - PLC Project Control
- Unknown Tag Detection based on Process Control technology
- Intrusion Detection methods:
    - Rule-based Intrusion Detection
    - ARP spoofing detection
    - IP protocol anomaly detection
    - TCP protocol anomaly detection

If a technology or method is disabled, the application does not monitor communications of assets using this technology or method. However, you can configure the settings of disabled technologies and methods (for example, add or edit rules).

The mode can be changed for the following technologies and methods:

- Network Integrity Control
- Command Control
- Asset activity detection

After the application is installed, all technologies and methods (except PLC Project Control and Unknown Tag Detection) are enabled by default. Learning mode is enabled by default for technologies and methods whose mode can be changed.

To change the state and/or mode of technologies and methods:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. Select the **Settings** section and go to the **Technologies** tab.

   You will see a list of technologies and methods whose states and modes can be changed.

   > If the states or modes of technologies and methods cannot be changed at the current time, the toggle switches in the list are not available (the **No data** value is displayed in the mode selection fields). 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.

3. Use the toggle switches on the left to enable or disable the use of relevant technologies and/or methods. To enable or disable all technologies and methods simultaneously, use the **Activate all** or **Deactivate all** button.

4. 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.

5. If Network Integrity Control technology, Command Control technology, or the Asset Activity Detection method are enabled, select the necessary mode. To do so, in the drop-down list on the right of the name of the technology or method, select one of the following options:

   - **Learning** – to apply the technology or method in learning mode.

   - **Monitoring** – to apply the technology or method in monitoring mode.

   To change the mode of all enabled technologies and methods simultaneously, use the **Mode** drop-down list.

6. After selecting a mode, wait for the changes to be applied. Until the mode is changed, the drop-down list displays the *Changing* status.

   If you selected different modes for enabled technologies and methods, the **Mode** drop-down list displays the **Mixed** value.

Using the Kaspersky Industrial CyberSecurity for Networks API

Kaspersky Industrial CyberSecurity for Networks has an application programming interface (API) that contains a set of functions for use in external applications. The Kaspersky Industrial CyberSecurity for Networks API provides gRPC methods for receiving data from Kaspersky Industrial CyberSecurity for Networks and for sending data to the application.

API methods for Kaspersky Industrial CyberSecurity for Networks let you perform the following actions:

- Receive asset information from the assets table.

- Receive information about events of Kaspersky Industrial CyberSecurity for Networks.

- Send events to Kaspersky Industrial CyberSecurity for Networks.

- Receive data on tags.

- Sign up for notifications about reading and writing of the values of tags.

- Receive data on the current security policy.

The Kaspersky Industrial CyberSecurity for Networks API is supplied as a package containing a set of proto files. This package is included in the application distribution kit. Proto files can be compiled into source code that enables execution of RPC requests to Kaspersky Industrial CyberSecurity for Networks.

Documentation for the Kaspersky Industrial CyberSecurity for Networks API is published in Online Help format on the Kaspersky Online Help page. This documentation serves as the Developer's Guide. The Developer's Guide describes the application programming interface used for RPC requests to Kaspersky Industrial CyberSecurity for Networks. The Developer's Guide also provides sample code and detailed descriptions of called elements that are available in the Kaspersky Industrial CyberSecurity for Networks API. The Developer's Guide for the Kaspersky Industrial CyberSecurity for Networks API is intended for professionals who are familiar with the Python programming language and with the principles of developing applications using an API.

The Kaspersky Industrial CyberSecurity for Networks API uses the Google™ RPC network interaction protocol. The Google RPC library supports a wide range of programming languages.

Certificates for secure connection through the API

Client applications that connect to Kaspersky Industrial CyberSecurity for Networks Server through the API establish a secure connection using client certificates and the gRPC server certificate.

During the application installation process, the following keys and certificates are created:

- gRPC server certificate (the file named product_facade_grpc_server.crt).

  This certificate is used by client applications for Server authentication. The Server uses this certificate to establish a connection with client nodes.

- Root certificate of the gRPC server (the file named product_facade_grpc_ca.crt).

  This certificate is used by the administrator to create client certificates. Client applications use this certificate to confirm the authenticity of their certificates (as part of the certificate chain).

- Private key of the gRPC server (the file product_facade_grpc_ca.key).

  This private key is used by the administrator to create client certificates.

By default, the specified files are located in the folder /var/opt/kaspersky/kics4net/public_certs/. Access to this folder is granted to a user with root privileges as well as to users of the kics4net group.

To connect to the gRPC server, the client application must use the following certificates and keys:

- gRPC server certificate (the file named product_facade_grpc_server.crt).

  This certificate, which is created during installation of the application, is required for Server authentication.

- Certificate chain (the file client.crt).

  This certificate chain is used by the client application for authentication. The certificate chain includes a client certificate authenticated by the root certificate of the gRPC server, and the chain of certificates up to the root certificate of the gRPC server.

- Private key of the client (the file client.key).

  This private key is used by the client application during authentication.

The administrator must create certificates and keys to be used by client applications (hereinafter also referred to as "client certificates"). Each client certificate must be created in the name of the computer that will connect to the Kaspersky Industrial CyberSecurity for Networks Server through the API.

For information on using client certificates to establish a connection with the Kaspersky Industrial CyberSecurity for Networks Server through the API, please refer to the documentation for the Kaspersky Industrial CyberSecurity for Networks API.

Creating client certificates for connection through the API

To create client certificates:

1. Obtain from the user the name of the computer for which a client certificate must be created.

2. Obtain from the user a certificate signing request for the client computer.

   If you must independently create a private key for the client and CSR, you can use the OpenSSL tool. To do so, enter the following commands:

   ```
   openssl genrsa -des3 -out client.key 4096
   openssl req -new -key client.key -out client.csr
   ```

3. Create a certificate based on the obtained CSR using the root certificate and private key of the gRPC server. The certificate must be created in the name of the client computer that will be used to establish a connection (see step 1).

   For the created certificate, in the settings of the OpenSSL tool specify the certificate validity period in days (the `days` setting) and the serial number of the certificate (the `set_serial` setting). Example command for creating a certificate:

   ```
   openssl x509 -req -days 365 -in client.csr \
   -CA product_facade_grpc_ca.crt \
   -CAkey product_facade_grpc_ca.key \
   -set_serial 01 -out client.crt
   ```

4. Create a certificate chain that includes the root certificate of the gRPC server into the final client certificate.

   If you are using intermediate certificates, they must also be included in the chain. To create a certificate chain, enter the following command:

   ```
   cat product_facade_grpc_ca.crt >> client.crt
   ```

5. Provide the following certificates and keys to the user of the client application:

   - gRPC server certificate (the file named product_facade_grpc_server.crt).

   - Private key of the client (the file client.key).

     This file needs to be sent only when the private key of the client has been created by the administrator.

   - Certificate chain or client certificate (the file client.crt).

     This file includes the certificate chain, beginning with the signed client certificate and ending with the root certificate of the gRPC server.

   - If a client certificate must be sent separately, also send the root certificate of the gRPC server (the file product_facade_grpc_ca.crt) and all intermediate certificates if they are being used.

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.

You can track the more significant changes in the system by viewing data in the **Assets** and **Events** sections. If you need to view more detailed information (for example, about assets requiring attention), you can proceed to other sections of the application web interface or open a tooltip.

> To view data in online mode, you can also use the Tags section, which lets you view tags with process parameter values and monitor the current state of Kaspersky Industrial CyberSecurity for Networks.

Information in the Assets block

The **Assets** block of the **Dashboard** section displays information about devices that are included in the list of known assets.

This section 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 **Assets** section. The number of assets of the specific category is indicated under the icon of each category. If the list of assets contains devices requiring attention, the warning icon is displayed on the category icons of these devices.
- List of categories with assets requiring attention. This data is displayed in the middle part of the **Assets** section if such devices are present. The space used for displaying graphical elements is limited by the size of the **Assets** section.

The application determines that a device requires attention in any of the following cases:

- The asset has the *Authorized* status and a security state other than *OK*.
- The asset has the *Unauthorized* status.

If there are assets requiring attention, the following information is displayed for each category in the list:

- Line containing the category icon, text comment, and link containing the number of assets requiring attention.
- Line containing the graphical elements representing the assets. This line is displayed if there is sufficient free space in the **Assets** section. The number of graphical elements in the line depends on the current size of the web browser window. If there are more devices requiring attention 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 representing assets contain the following information:

- Device name.
- Device status. This is displayed as an icon if the device has the *Unauthorized* status.
- Asset 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*, *Warnings* or *Critical events* states.

The graphical elements are displayed in the following order:

1. Assets assigned the *Unauthorized* status.
2. Assets with the *Critical events* security state.
3. Assets with the *Warnings* security state.

Viewing detailed information about assets

To view detailed information about assets, you can proceed to the assets table by using the management elements in the **Assets** block of the **Dashboard** section. The following options are provided:

- Receive information about all assets of the selected category.
- Receive information about assets that require attention and belong to a specific category.
- Receive information about an asset requiring attention.
- Receive information about all known assets.

To go to the assets table and view information about all assets in the selected category:

In the upper part of the **Assets** section, click the icon of the relevant category.

The **Assets** section opens in the web browser window. The assets table will be filtered based on the select category of assets.

To proceed to the assets table and view information about devices that require attention and belong to a specific category:

In the list of categories containing devices requiring attention, click the link containing the number of devices of the relevant category (this link is displayed at the end of the line containing the category icon and text comment **requiring attention**).

The **Assets** section opens in the web browser window. The assets table will be filtered based on the IDs of assets that require attention and belong to the specific category.

> The assets table is filtered based on the IDs of those assets that were displayed in the **Assets** block when you proceeded to the assets table. After you switch to the assets table, the filter settings are not updated. If you want to view the current number of assets requiring attention, you can go to the **Dashboard** section again.

To go to the assets table and view information about an asset requiring attention:

In the **Assets** section, click the graphical element that represents the relevant asset.

The **Assets** section opens in the web browser window. The assets table will be filtered based on the asset ID.

To go to the assets table and view information about all devices that are known to the application:

In the **Assets** block, click the **Show all assets** button.

The **Assets** section opens in the web browser window. The assets table will display the assets that satisfy the filter settings that were previously defined in the assets table.

Searching assets and proceeding to the Assets section

When viewing information in the **Assets** block of the **Dashboard** section, you can search for assets in the assets table.

To find the relevant assets:

1. In the **Assets** block, enter your search query into the **Search assets** field.
2. Click the **Search** button.

   The **Assets** section opens in the web browser window. The assets table will display the assets that meet the search criteria.

Information in the Events block

The **Events** block of 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 section displays the following elements:

- Histogram of events and incidents for the selected period. This data is displayed in the upper part of the **Events** section. 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 **Events** section.

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 severity 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 *Informational* severity level.
- Yellow. This color is used for events and incidents with the *Warning* severity level.
- Red. This color is used for events and incidents with the *Critical* 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. The following periods are available for building a histogram:

- 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 one-day intervals.

List of events and incidents

The list of events and incidents in the **Events** block 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 **Events** block.

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: *Informational*, *Warning*, or *Critical*.

Incidents in the list are marked with the 📁 icon.

Selecting a period for displaying a histogram

You can select the relevant period for generating a histogram of registered events and incidents in the **Events** block in the **Dashboard** section.

To generate a histogram for the relevant period:

In the **Events** block, click one of the following buttons:

- **1h** – if you want to generate a histogram for the last hour.
- **12h** – if you want to generate a histogram for the last 12 hours.
- **24h** – if you want to generate a histogram for the last 24 hours.
- **7d** – if you want to generate a histogram for the last seven days.

Data for the selected period will be displayed on the histogram showing the distribution of events and incidents.

Viewing detailed information about events and incidents

To view detailed information about events and incidents, you can proceed to the events table by using the management elements in the **Events** block of the **Dashboard** section. The following options are provided:

- Receive information about an event or incident that is displayed in the **Events** block.
- Receive information about all events and incidents.

*To view detailed information about an event or incident displayed in the list of the **Events** section:*

In the **Events** block, click the relevant event or incident.

In the web browser window, the **Events** section opens. The events table will apply a filter 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.

To view detailed information about all events and incidents:

In the **Events** block, click the **Show all events** button.

In the web browser window, the **Events** section opens. The events table displays the events and incidents that meet the filter settings that were previously defined in the events table.

Searching events and incidents and proceeding to the Events section

When viewing information in the **Events** block of the **Dashboard** section, you can search events and incidents in the events table.

To find relevant events and incidents:

1. In the **Events** block, enter your search query into the **Search events** field.
2. Click the **Search** button.

   In the web browser window, the **Events** section opens. The events table displays the events and incidents that meet the search criteria.

Working with the network map

The network map is a visual representation of monitored communications between industrial network devices. You can use the network map to view information about communication between devices during various time periods.

The following objects may be displayed on the network map:

- Nodes. These objects designate the sources and destinations of network packets within detected communications.
- Asset groups. These objects correspond to groups in the asset group tree. Groups contain nodes that represent the assets and child groups embedded in those groups.
- Links. These objects represent connections between nodes.

Nodes and links appear on the network map based on data received from traffic for a specific time interval. Asset groups are continually displayed.

If necessary, you can filter nodes and links. By default, the network map displays objects in online mode with a defined filtering period of one hour.

Objects requiring attention are visually distinguished on the network map. The application considers the following to be objects requiring attention:

- Node associated with unprocessed events that have the *Warning* or *Critical* severity, or node that represents an asset with the *Unauthorized* status.
- Link associated with events that have the *Warning* or *Critical* severity. 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 assets requiring attention, or whose nodes have links requiring attention. This includes objects within the group and within any child group of all nesting levels.

Nodes on the network map

Nodes on the network map can be of the following types:

- A device that is known to the application (an asset). This type of node represents an asset that is listed in the assets 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 assets table. Such a node may appear on the network map, for example, if network packets are sent using the `ping` command to the address of a non-existent device. Nodes of unknown devices are displayed individually if their total number does not exceed 100 (according to the current filter settings on the network 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.

Displayed information on nodes representing assets

The following information is displayed for nodes representing assets when the network 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).
- Asset status icon:
  - ✓ – the asset has the *Authorized* status.
  - ⚠ – the asset has the *Unauthorized* status.
  - ⬇ – the asset has the *Archived* status.

- The thick line on the left border of a node has one of the following colors depending on the asset's security state:
  - Green signifies the *OK* security state.
  - Yellow signifies the *Warning* security state.
  - Red signifies the *Critical* security state.
- The ✣ icon signifies that the router indicator has been set for the asset.

If an asset 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 is displayed for nodes representing unknown devices when the network 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 unknown devices.
- ❓ icon for the status of unknown devices.

Nodes that represent unknown devices have a gray background.

Displayed information on WAN nodes

The following is displayed for WAN nodes when the network map scale is maximized:

- Node name: **WAN**.
- WAN node icon 🖧.

Groups of assets on the network map

Groups from the asset group tree may be displayed in collapsed or expanded states on the network map.

Displayed information on collapsed groups

If a group is collapsed, the following is displayed when the network map scale is maximized:

- Group name.
- Number of assets that satisfy the current filter settings on the network map. This number includes assets within the group and within its child groups in all nesting levels.
- Number of child groups in all nesting levels.

If a group contains assets or links requiring attention (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 assets included in this group, and the child groups of the next nesting level. Of the assets included in the group, only the assets that meet the current filter settings on the network map are displayed.

If a group contains assets or links requiring attention (including in child groups of any nesting level), the window has a red background.

Links on the network map

Links on the network map are identified based on detected network packets in which the source and destination addresses can be correlated to the addresses of nodes.

Each link shows two sides of communication. A side of communication in a link may be one of the following objects on the network map:

- Node that represents one asset.
- Collapsed group, if the link shows communication with one or more assets in this group.
- Consolidated node of unknown devices, if the link shows communication with one or more unknown devices of this node.

Depending on the severity of events registered when communications are detected, the link may have the following colors:

- Gray – the communication did not cause event registration, or only events with the *Informational* severity level were registered.
- Red – the communication caused the registration of events with the *Warning* or *Critical* severity level.

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.

Viewing details about objects

Detailed information about objects presented on the network 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 asset, the details area displays the same information that is displayed in the assets table.
- If a node represents one unknown device, the details area displays the MAC address and/or IP address of the device.

- 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. 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. 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 assets whose addresses are included in the listed subnets are excluded from the asset group.
  - **Subnets** – section containing a list of subnet masks by which devices of an external network are identified.

The following information is displayed for groups:

- Number of assets and groups within the selected group and its child groups of all nesting levels.
- Path to the group in the asset group tree. If a group is in the top level of the hierarchy, **Top-level group** is displayed.
- Information about the number of objects requiring attention 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 importance 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 asset or a node of an unknown device, the section displays the name or address of the asset/device, category, and address information (for a known asset, address information is provided only for those network interfaces that were used during the communication).
  - If the side of communication is a collapsed group, the section displays the name of the group and the number of assets 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.
- If one of the sides of communication is a collapsed group, you will see the number of links that are designated by the selected link:
  - **Total links** – total number of links with assets of the collapsed group.
  - List showing the quantitative distribution of links based on the severity of their associated events (including the number of links not associated with any event). Next to list items are links for viewing detailed information about the items. You can click the **To assets** link to go to the **Assets** section and filter assets associated with links. You can click the **To events** link to go to the **Events** section and filter events associated with links.

- 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 network map scale and positioning

The network 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 network map display area.

You can change the positioning of the network map by moving it around the screen.

You can use the following functions when working with the network map:

- Changing the network map scale

  To change the scale of the network 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 map reduces the amount of information that is displayed in 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 (asset), the upper-right corner displays the asset status as a triangle in one of the following colors:
    - Green signifies that the asset has the *Authorized* status.
    - Red signifies that the asset has the *Unauthorized* status.
    - Gray signifies that the asset 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 requiring attention. The triangle has one of the following colors:
    - Green means that the group does not contain objects requiring attention.
    - Red means that the group contains objects requiring attention.

- Changing the positioning of the network map

  If necessary, you can change the positioning of the network map manually or automatically. Automatic positioning lets you move the network map and change its scale in such a way to display all nodes that satisfy the defined filter settings, and all expanded groups.

  To manually position the network map:

  1. Position the mouse cursor over any part of the network map that is not occupied by objects.
  2. Click and hold the left mouse button to drag the network map image.

  To automatically position the network map:

  Click the ⤢ button in the toolbar located in the left part of the network map display area.

  The positioning and scale of the network map will change to display all nodes and expanded groups.

Collapsing and expanding groups

You can collapse and expand asset groups on the network map. Collapsed groups are displayed as icons similar to nodes. Expanded groups are displayed as windows containing their embedded nodes and other groups.

To expand groups on the network map:

1. On the network map, select one or more nodes collapsed groups.

   To select multiple collapsed groups, perform 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 the ⤢ button in the toolbar located in the left part of the network map display area (the button is available if at least one collapsed group is selected).

To collapse expanded groups on the network map, perform one of the following actions:

- If you want to collapse one expanded group, click the ⤡ button in this groups' window title.
- If you want to collapse all expanded groups on the network map, click the ⤡ button in the toolbar located in the left part of the network map display area (the button is available if at least one group is expanded).

Moving nodes and groups to other groups on the network map

You can change the location of nodes and groups in the asset group tree by dragging objects on the network map. After being moved, nodes and groups change their location in the asset group tree just as when adding assets to a group and removing assets 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 a web browser using the account credentials of a user with the Administrator role.

2. In the **Network map** section, select the relevant nodes of assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.

3. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.

4. Move the cursor over one of the selected objects (group or node representing a known asset).

5. 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.

6. In the prompt window, confirm movement of the selected objects.

Pinning and unpinning nodes and groups

By default, the location of nodes and collapsed groups is not pinned on the network map. Before the locations of nodes and collapsed groups are pinned, they may be automatically arranged for optimal display of other objects.

Objects that are included in groups can be moved only within the confines of their respective groups. Other objects may occupy any space on the network map except the space occupied by expanded groups.

Nodes and groups are pinned when their location is changed manually or automatically. You can also pin the current location of displayed nodes and collapsed groups within the confines of one group or on the entire network map.

After the location of a node or collapsed group is pinned, the 📌 icon appears in the upper-right corner of this element. The icon is no longer displayed when the network map scale is reduced to 25% or less.

The location of a pinned node or pinned group is retained. If a pinned node disappears from the network map (for example, after a filter is applied), this node will be displayed in the same location the next time it appears.

To pin the location of displayed nodes and collapsed groups, perform one of the following actions:

- If you want to pin the location of all displayed nodes and collapsed groups on the network map, click the 📌 button in the toolbar located in the left part of the network map display area (the button is available if there are unpinned objects on the network map).
- If you want to pin the location of displayed nodes and collapsed groups in the window of an expanded group, click the 📌 button in the expanded group's window title (the button is available if there are unpinned objects within the window of the group).

To unpin displayed nodes and collapsed groups, perform one of the following actions:

- If you want to unpin one node or one collapsed group, click the 📌 icon in the upper-right corner of the node or collapsed group.
- If you want to unpin all displayed nodes and collapsed groups on the network map, click the 📌 button in the toolbar located in the left part of the network map display area (the button is available if there are pinned objects on the network map).
- If you want to unpin displayed nodes and collapsed groups in the window of an expanded group, click the 📌 button in the expanded group's window title (the button is available if there are pinned objects within the window of the group).

Manually changing the location of nodes and groups

You can manually change the location of nodes and groups on the network map by using the arrangement method that is most convenient 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 map, select one or multiple objects representing nodes and/or collapsed groups.

   To select multiple nodes and/or collapsed groups, 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 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 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 automatically arrange the following objects:

- All displayed nodes and groups at the top level of the hierarchy within the group tree.
- All displayed nodes and groups in an expanded group.
- Selected nodes and collapsed groups.

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.

To automatically arrange all displayed nodes and groups that are located at the top level of the hierarchy in the group tree:

1. In the toolbar located in the left part of the network map display area, click one of the following buttons (the buttons are available if there are nodes or groups displayed on the network map):

   - If you want to radially arrange the objects, click the ≡ button.
   - If you want to align the objects according to the grid, click the ▦ button.

   A window with a confirmation prompt opens.

2. In the prompt window, confirm the change in location of the objects.

To automatically arrange only the displayed nodes and groups within an expanded group:

1. Expand the relevant group on the network map.
2. In the title of the expanded group's window, click one of the following buttons (the buttons are available if there are displayed nodes or groups within the group):
   - If you want to radially arrange the objects, click the ≡ button.
   - If you want to align the objects according to the grid, click the ▦ button.

   A window with a confirmation prompt opens.

3. In the prompt window, confirm the change in location of the objects.

To automatically arrange only the selected nodes and collapsed groups on the network map:

1. On the network map, select multiple nodes and/or 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 objects.
   - Hold down the **`CTRL`** key and use your mouse to select the relevant objects.
2. In the toolbar located in the left part of the network map display area, click one of the following buttons (the buttons are available if at least three objects with common links are selected):
   - If you want to radially arrange the objects, click the ≡ button.
   - If you want to align the objects according to the grid, click the ▦ button.

   A window with a confirmation prompt opens.

3. In the prompt window, confirm the change in location of the objects.

Filtering nodes and links by time of communication

You can configure filtering of nodes and links to display only the ones that communicated during the specified time period.

You can select the filtering period by using the time scale displayed in the lower part of the **Network map** section. The following elements are displayed on the time scale:

- Time scale start date and time.

- Periods when events with the *Critical* and *Warning* severity levels 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 end of the time scale.
- 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 period correlated to the current moment:

1. Click the **Now** button on the right of the time scale.

   > You can also use the mouse to move the period to the right part of the time scale.

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 window for selecting the period duration by using the button showing the current period duration above the yellow band of the period, select the relevant option (**Hour**, **Day**, **7 days**), and click **OK**.

   The network map shows only those 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**
      - **Month**
      - **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 relevant period. To do so, perform one of the following actions:

- 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 window for selecting the period duration by using the graphical element above the yellow band of the period, select the relevant option (**Hour**, **Day**, **7 days**), and click **OK**.

> You can also use the mouse to move the period to the relevant place on the time scale.

The network map shows only those nodes and links for which communications were detected during the currently defined period.

Filtering nodes on the network map

By default, the network map displays all nodes that have communicated during the defined time period. To limit the number of nodes displayed on the network map, you can use the following functions:

- Filtering by asset status

To filter nodes on the network map based on the statuses of assets:

1. In the toolbar located above the network map, open the **Asset statuses** drop-down list.

   You will see a list containing the names of statuses for assets 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 assets that need to be displayed on the network map.

3. Click **OK**.

The network map displays only those nodes that represent assets with the selected statuses.

- Filtering by asset security state

To filter nodes on the network map based on the security states of assets:

1. In the toolbar located above the network map, open the **Asset states** drop-down list.

   You will see a list containing the names of security states for assets (**OK**, **Warning**, **Critical events**).

2. In the drop-down list, select the check boxes for the security states of nodes that need to be displayed on the network map.

3. Click **OK**.

The network map displays only those nodes that represent assets with the selected security states.

- Filtering by asset category

To filter nodes on the network map based on the categories of assets:

1. In the toolbar located above the network map, open the **Asset categories** drop-down list.

   You will see a list containing the names of categories for known assets, as well as individual categories for unknown devices and WAN nodes.

2. In the drop-down list, select the check boxes for those categories of assets that need to be displayed on the network map.

3. Click **OK**.

The network map displays only those nodes that represent the selected categories of assets.

After applying a filter, the network map displays only those nodes that satisfy the defined filter settings. In addition, for a node to be displayed on the network map, it must have a connection (link) with another displayed node. If the defined filter settings cause the network map to not display all nodes with which a node has interacted, this node is also not displayed on the network 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 map to display all nodes associated with filtered nodes. Together with nodes that satisfy the defined node filter settings, the network map will also display all nodes with which interactions have occurred (irrespective of the defined filter settings).

For example, if node filtering by **PLC** category is enabled and you have enabled the display of linked nodes, the network map will display all nodes with which **PLC** category assets have communicated. If the display of linked nodes is disabled, the network map will display nodes of only those **PLC** category assets that have communicated with each other.

To enable or disable the display of nodes associated with filtered nodes:

Use the **Linked assets** toggle switch in the toolbar located above the network map.

Filtering links on the network map

By default, the network map displays all links for which communication was detected during the defined time period. To limit the number of links displayed on the network map, you can use the following functions:

- Filtering based on event severity ?

  To filter links on the network map based on event severity levels:

  1. In the toolbar located above the network map, open the **Link severity levels** drop-down list.

     You will see a list containing the names of the severity levels of events (**Informational**, **Warning**, **Critical events**), as well as the **No events** item that lets you filter connections for which no events have been 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 map displays only those links associated with events that have the selected severity levels.

- Filtering by communication protocols ?

To filter links on the network map based on the protocols of communications:

1. In the toolbar located above the network map, open the **Protocols** 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 map displays only those links in which the selected protocols were 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 map based on the layers of the OSI network model:

1. In the toolbar located above the network 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 those OSI model layers whose links need to be displayed on the network map.

3. Click **OK**.

The network map displays only those links that are associated with the selected OSI model layer.

Saving and loading network map display settings

The application lets you save the current network map display settings. A set of saved display settings is called a *view*. You can use views to apply their saved settings on the network map (for example, to quickly restore the display settings after making some changes, or to work with the network map on a different computer).

When a network map view is saved, the following display settings are saved:

- Location of pinned nodes and groups
- Scale and positioning of the network map
- Filtering of nodes
- Filtering of links

The application can save and use no more than 10 groups of settings providing different views of the network map.

Only users with the Administrator role can manage the list of network 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 map views, you can use the following functions:

- Adding a new view while saving the current network map display settings

  To add a new view and save the current network map display settings in this view:

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
  2. In the **Network map** section, configure the network map display settings.
  3. Click the **Manage views** button.

     The **Configure network map views** window appears.
  4. Click the **Add current** button.
  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 map display settings

  To update a view and save the current network map display settings in this view:

  1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
  2. In the **Network map** section, configure the network map display settings.
  3. Click the **Manage views** button.

     The **Configure network map views** window appears.
  4. Select the view in which you want to save the current network 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 map view

To rename a view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, click the **Manage views** button.

   The **Configure network map views** window appears.
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 map view

To delete a view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser using the account credentials of a user with the Administrator role.
2. In the **Network map** section, click the **Manage views** button.

   The **Configure network map views** window appears.
3. Select the view that you want to delete.
4. Click the **Remove** 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 map

To apply the settings saved in a view on the network map:

1. In the **Network map** section, click the **Manage views** button.

   The **Configure network map views** window appears.
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.

Resetting the defined filter settings on the network map

You can reset the defined settings for filtering nodes and links to their default state.

To reset the defined filter settings on the network map:

In the toolbar located above the network map, click the **Clear filter** button (this button is displayed if filter settings have been defined).

The network map will display all nodes and links for which communications were detected during the currently defined period.

Searching nodes on the network map

You can search nodes on the network map based on information about these nodes. This search will involve all nodes that meet the current filter settings, including those located in collapsed groups or outside of the displayed part of the network map.

For nodes representing known assets, the search is performed in all columns of the assets table except the following columns: **Status**, **Security state**, **Last seen**, **Last modified** and **Creation date**. The search is also performed in the values of custom fields for assets.

To find the relevant nodes on the network map:

1. 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 information:

   - 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.

2. To navigate between the found objects, use the arrow buttons in the right part of the **Search nodes** field. Arrow movements proceed in alphabetical order of the names of found objects. When moving to the next object, the network map is automatically positioned to display this object.

Viewing events associated with nodes of known assets

For nodes representing known assets on the network map, you can view the events associated with these assets. When events are loaded, they are automatically filtered based on the IDs of assets using the values of the MAC- and IP addresses specified for the assets.

The capability to load events is available if no more than 200 nodes on the network map are selected. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To view events associated with assets:

1. On the network map, select one or multiple objects representing nodes of known assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

   The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.

2. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.

3. Depending on which events you want to load, click one of the following buttons (the buttons are unavailable if the total number of assets in the selection exceeds 200):

   - **Show events** – if you want to view events with any status.
   - **Show unprocessed events** – if you want to view events with the *New* or *In progress* status.

   The **Events** section opens. The events table will apply a filter based on the IDs of assets corresponding to the selected nodes on the network map (the **Asset IDs** field appears in the toolbar). If you loaded events by using the **Show unprocessed events** button, events are additionally filtered by the **Status** column.

Viewing events associated with a link

You can view the events associated with links on the network map. When events are loaded, they are automatically filtered based on the IDs of events associated with the link, and based on the time period.

You can use the following methods to load events associated with links:

- Load events associated with a selected link. This method can be used for any link except links with the consolidated node of unknown devices.
- Load events associated with links to nodes in a collapsed group.

The application loads no more than 200 events associated with a link. If there are more events, the events with the highest severity and with the latest time of occurrence are selected first.

To view events associated with a link:

1. On the network map, select a link (except a link in which one of the sides of communication is a consolidated node of unknown devices).

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

2. Depending on which events you want to load, click one of the following buttons (the buttons are available if there are events associated with the link):

   - **Show events** – if you want to view events with any status.
   - **Show unprocessed events** – if you want to view events with the *New* or *In progress* status.

3. If more than 200 events associated with the link were registered during the time period defined on the network map, you will see a warning about the large number of events. In the prompt window, confirm whether you want to load events with the highest severity levels.

The **Events** section opens. The events table will apply a filter based on the IDs of events and the time period defined on the network map. If you loaded events by using the **Show unprocessed events** button, events are additionally filtered by the **Status** column.

To view events associated with links of nodes in collapsed groups:

1. On the network map, select the link showing interactions with nodes in the collapsed group.

   The details area appears in the right part of the web interface window. The **Total links: <number>** settings group contains a list of the maximum severities of events in links to nodes of the collapsed group. For each severity level, the number of links with this severity is displayed. Only the severities of links to nodes of the collapsed group are shown. If there are links that are not associated with any events, **No events** is displayed with the number of such links.

2. Load events by using the **To events** link in the row containing the relevant severity.

   You can load the following events:

   - For the **Critical** severity level, events associated with links that have **Critical** severity are loaded.
   - For the **Warning** severity level, events associated with links that have a **Warning** or **Critical** severity are loaded.
   - For the **Informational** severity level, events associated with links that have an **Informational**, **Warning** or **Critical** severity are loaded.

3. If more than 200 events associated with links that have the selected severities were registered during the time period defined on the network map, you will see a warning about the large number of events. In the prompt window, confirm whether you want to load events with the highest severity levels.

The **Events** section opens. The events table will apply a filter based on the IDs of events and the time period defined on the network map.

Viewing information in the assets table for selected nodes

For nodes representing known assets on the network map, you can view information in the assets table. The assets table automatically applies a filter based on the IDs of known assets.

The capability to load information is available if no more than 200 nodes representing known assets are selected. You can select the relevant nodes individually or as part of collapsed groups that include the relevant assets. When a collapsed group is selected, all assets in the child groups of any nesting level are also included in the asset selection.

To view information about assets in the assets table:

1. On the network map, select one or multiple objects representing nodes of known assets and/or collapsed groups.

   To select multiple nodes and/or groups, 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.

The details area appears in the right part of the web interface window. The details area shows the total number of selected nodes and groups while also showing the quantitative distribution of selected objects by type.

2. If the selected objects belong to different types or categories of devices, you can exclude certain types of objects (for example, nodes of devices that are unknown to the application) or categories (for example, PLC). To do so, clear the check box next to the name of the category or type.
3. Depending on the number of selected objects, click the **Show asset** or **Show assets** button (the **Show assets** button is not available if the total number of known assets in the selection exceeds 200).

The **Assets** section opens. The assets table will apply a filter based on the IDs of assets corresponding to the selected nodes on the network map.

Viewing information in the assets table for a selected link

For links on the network map, you can view information about known assets involved in communications. Proceed to the assets table to load information. The assets table automatically applies a filter based on the IDs of known assets.

You can view information in the assets table only for links to nodes in collapsed groups.

The application loads no more than 200 assets associated with links to nodes in collapsed groups. If there are more assets, the assets associated with links with the highest severity are selected first.

To view information about assets associated with links to nodes in collapsed groups:

1. On the network map, select the link showing interactions with nodes in the collapsed group.

   The details area appears in the right part of the web interface window. The **Total links: <number>** settings group contains a list of the maximum severities of events in links to nodes of the collapsed group. For each severity level, the number of links with this severity is displayed. Only the severities of links to nodes of the collapsed group are shown. If there are links that are not associated with any event, **No events** is displayed with the number of such links.

2. Load asset information by using the **To assets** link in the row containing the relevant severity.

   You can load the following asset information:

   - For the **Critical** severity level, you can load information about assets associated with links that have **Critical** severity.
   - For the **Warning** severity level, you can load information about assets associated with links that have a **Warning** or **Critical** severity.
   - For the **Informational** severity level, you can load information about assets associated with links that have **Informational**, **Warning**, or **Critical** severity.
   - For the **No events** severity level, you can load information about assets associated with links that have any severity.

3. If the total number of known assets in the selection exceeds 200, you will see a warning about the large number of assets. In the prompt window, confirm whether you want to load assets associated with links that have the highest severity levels.

The **Assets** section opens. The assets table will apply a filter based on the IDs of assets.

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 system event types that are assigned the codes 8000000000, 8000000001, 8000000002 and 8000000003.

Event correlation rules are embedded in the application and are applied regardless of the security policy loaded in the Console or applied on the Server.

> 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 and relays information about them to external systems according to the settings defined for registering event types. You can configure these settings in the Console on the **Configure events** tab. For configuration information, please refer to the Configuring events section.

The settings for storing events and incidents are configured in the **Manage logs** window of the Application Console. By default, the database will store 100000 records for 365 days. If the number of records or the retention period exceed the specified maximum values, the oldest records are deleted. When necessary, you can change the number of stored records as well as their retention period.

The application saves events and incidents in the database on the Server.

> Deleting or modifying any file in DBMS folders can disrupt the operation of the application.

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** section displays detailed information about events and incidents and provides the capability to download information from the Server database for any period.

Event severity levels

Events and incidents in Kaspersky Industrial CyberSecurity for Networks are classified according to the following severity levels:

- *Informational* (marked with the ⓘ icon).

  Informational events and incidents contain reference information. These events usually do not require an immediate response.

- *Warning* (marked with the ⚠ icon).

  Warnings and incidents contain information that requires attention. These events may require a response.

- *Critical* (marked with the ❗ icon).

  Critical events and incidents contain information that may have a critical impact on the industrial process. These events require an immediate response.

You can define severity levels for custom event types. The severity levels for system event types (including events in incidents) are assigned by the application automatically.

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 external systems using Kaspersky Industrial CyberSecurity for Networks API methods.

- *Asset management* (AM)

  This technology is used to register events associated with detection of device information in traffic (for example, an event for the detection of a new IP address for a device).

You can assign the *Deep Packet Inspection* or *External* technology for custom event types. The application automatically assigns technologies for system event types.

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* (marked with the □ icon).

  This status is assigned to all events and incidents when they are registered in Kaspersky Industrial CyberSecurity for Networks.

- *In progress* (marked with the ⟳ icon).

  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* (marked with the ☑ icon).

  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 assets displayed in the assets table and on the network 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 in the **Events** section of the application web interface.

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 regenerate timeout 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.

You can perform the following operations when working with the table of events and incidents:

- Manage the display of events and incidents
- Filter events
- Search events

- Sort events
- Configure the table of registered events
- View event details
- Change the statuses of events
- View event information in the assets table
- Add markers
- Copy events to a text editor
- Export events to file
- Load traffic of events

The settings for displaying the events table (for example, the filter settings) are automatically saved for the current application user. The saved settings are applied the next time this user connects to the Server, provided that the connection is used by the same computer, web browser, and operating system user account.

Selecting events in the events table

In the events table, you can select events and incidents to view their information and to work with these events and incidents. When events and incidents are selected, the details area appears in the right part of the web interface window.

To find the relevant events and/or incidents:

- If you want to select one event or incident, select the check box next to this event or incident or use your mouse to select it.
- If you want to select multiple events and/or incidents, select the check boxes next to the events and/or incidents or select them by holding down the **CTRL** or **SHIFT** key. When multiple events and/or incidents are selected, the application checks their status and determines if there are events and incidents with the *New*, *In progress* and *Resolved* statuses among those selected.
- If you want to select all events and incidents that satisfy the current filter and search settings, perform one of the following actions:
  - Select any event or incident 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.

When multiple events and/or incidents are selected, the details area displays the total number of selected elements. However, embedded elements of collapsed incidents (events and other incidents) are not taken into account.

If you selected all events and incidents that satisfy the current filter and search settings, embedded elements of collapsed incidents are included in the total number of selected elements. The details area displays one of the following values:

- If 1000 or less events and incidents are selected, the precise number is displayed. In this case, the application checks the statuses of the selected events and incidents just as with other multiple selection methods.

- If more than 1000 events and incidents are selected, the number `1000+` is displayed. In this case, the application does not check the statuses of the selected events and incidents.

The title of the left-most column of the table shows a check box for the selection of events and incidents. Depending on the number of selected items in the table, the check box can have one of the following states:

- □ – all events and incidents that satisfy the current filter and search settings were not selected in the table. However, one event/incident or multiple events and/or incidents may be selected in the table by using the check boxes next to the events and incidents or by using the **`CTRL`** or **`SHIFT`** key.

- ☑ – all events and incidents that satisfy the current filter and search settings were selected in the table.

- ▣ – all events and incidents that satisfy the current filter and search settings were selected in the table, but then the check boxes for some of them were cleared. This state is also retained if the check boxes were cleared for all events and incidents selected in this way (due to the fact that the number of selected events and incidents may change).

If all events and incidents that satisfy the filter and search settings are selected, the number of selected elements may be automatically changed. For example, this may happen if new events or incidents are registered. It is recommended to configure the filter and search settings in such a way that ensures that only the relevant elements end up in the selection (for example, you can filter events by their IDs before selecting all events and incidents).

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 a tree structure with nested events and may be collapsed or expanded in the events table.

You can change the display mode when configuring the events table.

To expand or collapse rows containing information about embedded elements of an incident in tree display mode:

Click the ⊞ or ⊟ button in the cell containing the incident header.

Filtering events

To limit the number of events and incidents displayed in the events table, you can use the following functions:

- Filtering based on standard periods

When filtering based on a standard period, the events table is updated in online mode.

To configure filtering of events and incidents based on a standard period:

1. In the **Events** section, perform one of the following actions:
   - Open the **Period** drop-down list.
   - Click the filtering icon in the **Last seen** column.
2. In the drop-down list, select one of the standard periods:
   - **Last hour**
   - **Last 12 hours**
   - **Last 24 hours**
   - **Last 48 hours**
3. If table updates are disabled, in the opened window confirm that you agree to resume table updates.

The table will display events and incidents for the period you specified.

- Filtering based on a specified period ?

When filtering by a defined period, the table will no longer be updated. The table will display only the events and incidents whose date and time of last occurrence are within the specified period.

To configure filtering of events and incidents based on a specified period:

1. In the **Events** section, perform one of the following actions:
   - Open the **Period** drop-down list.
   - Click the filtering icon in the **Last seen** column.
2. In the drop-down list, select **Specify a period**.
3. If table updates are enabled, in the opened window confirm that you agree to suspend table updates.

   On the right you will see additional buttons that you can use to manually define the filtering period.
4. Click any of the buttons containing a date and time value in the **From** and **to** fields.

   The calendar opens.
5. In the field under the calendar on the left, specify the date and time for the start boundary of the filtering period. In the field under the calendar on the right, specify the date and time for the end boundary of the filtering period. If you want to remove the limit for the end boundary of the period, delete the value in the field under the calendar on the right.

   To enter a value into the field, you can select a date in the calendar (the current time will be specified for the selected date) or manually enter the necessary value. When the date and time are entered manually, you must enter the value in the format DD-MM-YYYY hh:mm:ss.
6. Click **OK**.

The events table will display events and incidents for the period you specified.

- Filtering based on table columns ?

You can configure filtering of events and incidents based on the values in all columns except the **End**, **Title**, and **Description** columns.

*To filter the events table by the **Start** column:*

1. In the **Events** section, click the filtering icon in the **Start** column.

   The calendar opens.

2. In the calendar, specify the date and time 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 want to remove the limit for one of the boundaries of the period, delete the value in the field under the calendar.

3. Click **OK**.

*To filter the events table by the **Severity**, **Technology**, **Status**, **Monitoring point** or **Marker** column:*

1. In the **Events** section, click the filtering icon in the relevant column.

   When filtering by severity level or technology, you can also use the corresponding buttons in the toolbar.

   The filtering window opens.

2. Select the check boxes opposite the values by which you want to filter events. You can select the **All** check box to select all values in the **Marker** and **Technology** columns.

3. Click **OK**.

*To filter the events table by the **Source** or **Destination** column:*

1. In the **Events** section, click the filtering icon in the relevant column.

   The filtering window opens.

2. In the **Including** and **Excluding** fields, in the drop-down lists select the types of address blocks that you want to include into the filter and/or exclude from the filter. You can select the following types of address blocks:

   - **IP address**
   - **Port number**
   - **MAC address**
   - **Application-level address**
   - **VLAN ID**
   - **Complex** – if you want to specify multiple address blocks of different types combined by the logical operator AND. To add different types of address blocks, use the **Add condition (AND)** button.

3. If you want to apply multiple filter conditions by address block type combined with the logical operator OR, in the filter window click the **Add condition (OR)** button and select the relevant types of addresses.

4. If you want to delete one of the created filter conditions, in the filter window click the ✕ icon located on the right of the field containing the drop-down list.

5. Click **OK**.

*To filter the events table by the **Protocol** column:*

1. In the **Events** section, click the filtering icon in the **Protocol** column.

   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**.

*To filter the events table by the **Total appearances**, **ID**, **Triggered rule** or **Event type** column:*

1. In the **Events** section, click the filtering icon in the relevant column.

   The filtering window opens.

2. In the **Including** and **Excluding** fields, enter the values for events and incidents that you want to include into the filter and/or exclude from the filter.

3. If you want to apply multiple filter conditions combined by the logical operator OR, in the filter window of the selected column click the **Add condition** button and enter the condition in the opened field.

4. If you want to delete one of the created filter conditions, in the filter window of the selected column click the 🗑 icon.

5. Click **OK**.

- Filtering based on the values in table cells

  You can filter the events table by the values in cells of any column except the following columns: **Start**, **Last seen**, **Title**, **Description** and **End**.

  To filter the table based on the values of settings in table cells:

  1. Select the **Events** section.

  2. In the events table, select the check box next to the event or incident whose setting you want to use as a filter.

     If you want to select multiple events and/or incidents, select the check boxes next to the events and/or incidents whose settings you want to use as a filter. You can also select multiple events and/or incidents by holding down the `CTRL` or `SHIFT` key.

     The details area appears in the right part of the web interface window. If multiple events and/or incidents are selected, the details area displays the total number of selected elements.

  3. In the events table, move your mouse cursor over a cell of the relevant column of one of the selected events or incidents.

  4. Right-click to open the context menu.

  5. In the context menu, select one of the following options:

     - **Show all events with this setting**, if one event or incident is selected.

     - **Show all events with these settings**, if multiple events and/or incidents are selected.

     > The **Show all events with this setting** or **Show all events with these settings** options are not available for selection if it is impossible to filter by column values.

     The table of registered events displays the events and incidents that have values in that same column matching the values of the selected events and/or 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.

Searching events

You can search events and incidents in the events table.

The search is performed in the columns containing characters (letters and/or numerals), except the **Start**, **Last seen**, **End** and **Total appearances** columns.

To find relevant events and incidents:

In the **Events** section, enter your search query into the **Search events** field. The search is initiated as you type characters in the search field.

The table displays the events and incidents that meet the search criteria.

When performing a search in tree display mode, incidents that meet the filtering criteria may be presented in the following variants:

- Displayed with all nested elements
- Only with the nested elements that also meet the search criteria

You can select the relevant display option for incidents by using the **Show embedded events when filtering** check box when configuring the table.

Resetting the defined filter and search settings in the events table

You can reset the defined filter and search settings in the events table to their default state.

To reset the defined filter and search settings in the events table:

In the toolbar in the **Events** section, click the **Clear filter** button (this button is displayed if the filter and/or search settings are defined).

Sorting events

You can sort events and incidents displayed in the **Events** section of the application web interface. You can sort by the values of any column except the **Description** column.

By default, table rows are sorted by the **Last seen** column in descending order of the dates and times when events last occurred. If the default sorting scheme is changed, the application stops updating events in the table.

To sort events and incidents:

1. In the **Events** section, click the header of the column by which you want to sort.
2. When sorting events by the **Destination** or **Source** column, in the drop-down list of the column header, select the address of the destination or source by which you want to sort.

   Depending on the values selected for display in these columns, you can select one of the following options:

   - IP address
   - Port number
   - MAC address
   - VLAN ID
   - Application-level address

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.

4. If table updates are enabled, in the opened window confirm that you agree to suspend table updates.

   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 showing the current sorting order: in ascending order or descending order of values.

Configuring the table of registered events

You can configure the following settings for displaying the events table:

- Display of the information panel
- Display of events included in incidents.
- Contents and order of columns displayed in the table.

To configure the settings for displaying the events table:

1. In the **Events** section, click the **Customize table** button.

   This will open a window for configuring how the events table is displayed.

2. If you want to enable display of the information panel showing the number of events with the *New* and *In progress* statuses, select the **Display information panel** check box.

3. In the **Display embedded lists** settings group, select the relevant mode for displaying events included in incidents:

   - **Flat**. In this mode, the events table displays all events without consideration of how events are nested in incidents.
   - **Tree**. In this mode, incidents are displayed as a tree of embedded events and other incidents. If you want the nested elements of incidents to be displayed regardless of the current filter and search settings, select the **Show embedded events when filtering** check box.

4. In the **Displayed table 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.

   The following settings are available for viewing:

   - **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 select 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.

- Severity

  This icon corresponds to the importance level of an event or incident.

- Source

  Address of the source of network packets (the abbreviated names for display in table cells are specified in parentheses):

  - IP address
  - Port number (P)
  - MAC address
  - VLAN ID (VID)
  - Application-level address

- Destination

  Address of the destination of network packets (the abbreviated names for display in table cells are specified in parentheses):

  - IP address
  - Port number (P)
  - MAC address
  - VLAN ID (VID)
  - Application-level address

- 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.

- 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.

5. If you want to change the order in which columns are displayed, select the name of the column that you want to move to the left or right in the table and use the buttons containing an image of the up or down arrows.

   For the **Start**, **Last seen** and **End** columns, you can also change the order in which the date and time are displayed. For the **Source** and **Destination** columns, you can change the order of the addresses of the senders and recipients of network packets. To do so, select the value that you want to move 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 **Events** section in the table in the order you specified.

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:

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.

Viewing information about assets associated with events

You can view information about assets associated with events in the assets table. The assets table is automatically filtered based on the IDs of assets using the values of the MAC- and IP addresses specified in events.

The capability to load information is available if no more than 200 events are selected, not including incidents (if incidents are selected, information is loaded for the first 200 events selected, including events of the selected incidents). The assets table displays information for no more than 200 assets associated with events.

To view information about assets in the assets table:

1. Select the **Events** section.
2. In the events table, select the events and/or incidents for which you want to view asset information.

   The details area appears in the right part of the web interface window.
3. Click the **Show assets** button.

   The **Show assets** button is not available if there are no incidents among the selected events and the number of selected events exceeds 200.

The **Assets** section opens. The assets table will be filtered based on the IDs of assets corresponding to the selected events.

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.

To assign the In progress status to events or incidents:

1. Select the **Events** section.
2. In the events table, select the events and/or incidents whose status you want to change. The selected events and/or incidents must have the *New* status.

   The details area appears in the right part of the web interface window.
3. Click the *In progress* button. The button is not available if the *In progress* or *Resolved* status is assigned to the selected events and incidents. If all events and incidents that satisfy the current filter and search settings are selected, and the number of selected elements is more than 1000, the application does not check their statuses. In this case, the *In progress* button is available.

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

To assign the Resolved status to events or incidents:

1. Select the **Events** section.
2. In the events table, select the events and/or incidents whose status you want to change. The selected events and/or incidents must have the *New* or *In progress* status.

   The details area appears in the right part of the web interface window.
3. Click the *Resolved* button. The button is not available if the *Resolved* status is assigned to the selected events and incidents. If all events and incidents that satisfy the current filter and search settings are selected, and the number of selected elements is more than 1000, the application does not check their statuses. In this case, the button with the *Resolved* status name is available.

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

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. 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 events is available if no more than 200 events are selected (including within the selected incidents).

To copy events to a text editor:

1. Select the **Events** section.
2. In the events table, select the events and/or incidents whose information you want to copy to a text editor.

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

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 you are copying one event or incident.

   - **Copy details of the selected events**, if you are copying multiple events and/or incidents.

5. Open any text editor.

6. Paste the details 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.

Exporting events to a file

You can export information about events and/or incidents to a CSV file. The information is exported from the columns that are currently displayed in the table.

To export information about events and/or incidents:

1. Select the **Events** section.

2. In the events table, select the events and/or incidents whose information you want to export to a file.

   > To export information about all events and incidents that satisfy the current filter and search settings, you can select all events and incidents in the table or use the **Export** button in the toolbar of the **Events** section. Clicking the **Export** button immediately starts the process for generating a CSV file.

   After events and/or incidents are selected, the details area appears in the right part of the web interface window.

3. Depending on the number of selected elements, click the **Export event** or **Export the selected events** button.

4. 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.

   This opens the standard web browser window for saving a file.

5. In the opened window, specify the name of the file and folder in which you want to save the file.

6. Save the file.

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). 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. Select the **Events** section.

2. In the events table, select the events and/or incidents whose traffic you want to load.

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

3. Depending on the number of selected elements, click the **Load traffic for the event** or **Load traffic for the selected events** button.

4. 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.

   This opens the standard web browser window for saving a file.

5. In the opened window, specify the name of the file and folder in which you want to save the file.

6. Save the file.

Monitoring process parameters

Kaspersky Industrial CyberSecurity for Networks displays process parameters in online mode.

The set of displayed process parameters is determined by Process Control tags. Only tags for which there are Process Control rules for them. You can generate lists of Process Control rules and tags in the Application Console on the **Process control** tab. For information on configuring Process Control, please refer to the Process Control section.

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.

You can view tags with the values of process parameters in the **Tags** section of the Kaspersky Industrial CyberSecurity for Networks web interface.

Viewing process parameters

To view a table containing the tags and values of process parameters:

Connect to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser and select the **Tags** section.

The web browser window will display a table containing the tags and their current values. The current tag processing rate is displayed in the **Tags** row in the upper part of the window.

Sorting tags when viewing process parameters

You can sort tags in the **Tags** section of the application web interface. Sorting is done by the **Tag name**, **ID** and **Description** columns.

To sort tags:

In the table of tags, click the header of the column by which you want to sort.

The table will be sorted by the selected column. Next to the header of the column you will see an icon displaying the current sorting order: in ascending order or descending order of values.

Application interaction with Kaspersky Security Center

This section contains information about configuring interaction between the application and Kaspersky Security Center, and about using Kaspersky Security Center functions to receive a license key, download updates for application modules and databases, and monitor events and the security state of the ICS.

To enable interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center, the following conditions must be fulfilled:

- The capability for application interaction with Kaspersky Security Center was added during installation of the Server. If this functionality was not added, add it.
- The Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center is installed in Kaspersky Security Center.
- 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). For detailed information on moving managed assets to administration groups, please refer to the Kaspersky Security Center Help system.

Connecting to the Console from Kaspersky Security Center

You can remotely connect to the Kaspersky Industrial CyberSecurity for Networks Console from the Kaspersky Security Center 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 access the Kaspersky Industrial CyberSecurity for Networks Console 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 **Assets** 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. If the Application Console is not running, start it.

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 Console.

To distribute a license key, you need to first add it to the Kaspersky Security Center Administration Server repository. You can add a license key to the Administration Server repository from a license key file.

Automatic distribution of a license key is possible if the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server is in the administration group in the **Managed devices** folder within the Kaspersky Security Center Administration Console tree. If the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server is not in the administration group, you need to add it.

For detailed information about licensing managed applications in Kaspersky Security Center and for descriptions of the actions required for automatic distribution of keys, please refer to the Kaspersky Security Center Help system.

Using the Kaspersky Security Center Administration Server as the source of updates

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.

To use the Kaspersky Security Center Administration Server as the source of updates for databases and application modules of Kaspersky Industrial CyberSecurity for Networks:

1. In the Kaspersky Security Center Administration Console, create and configure the "Download updates to the Administration Server repository" task.

   For detailed information on creating and using the "Download updates to the Administration Server repository" task, please refer to the Kaspersky Security Center Help system.

2. In the Kaspersky Industrial CyberSecurity for Networks Console, select the Kaspersky Security Center Administration Server as the source of updates.

3. Select the update run mode, or manually start an update if updates have already been downloaded to the Administration Server.

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** means the Kaspersky Industrial CyberSecurity for Networks event registration time in the time zone of the computer where Kaspersky Security Center is installed.
- **Asset** 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** 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.
- **Severity** means the importance level of the event based on how importance is typified by Kaspersky Security Center.
- **Registered** means the time at which the event was registered in the Kaspersky Security Center database.

You can configure the contents of fields displayed in the events table. For descriptions of how to add or remove fields in the tables, please refer to the Kaspersky Security Center Help system.

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. In the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center, configure the receipt of the relevant types of events for all event severity levels. For detailed

information on configuring the receipt of Kaspersky Security Center events, please refer to the Kaspersky Security Center Help system.

3. In the Kaspersky Industrial CyberSecurity for Networks Console, select the Configure events tab.
4. Add Kaspersky Security Center as a recipient of events. This recipient is added automatically if the capability to transmit events to Kaspersky Security Center is enabled when the security policy is created in Kaspersky Industrial CyberSecurity for Networks.
5. In the list, specify the types of events that you want to send to Kaspersky Security Center. If a recipient was added automatically for Kaspersky Security Center, transmission of all system types of events with the *Critical* severity is enabled by default for this recipient.
6. In the **Manage security policy** menu in the Application Console window, apply the security policy.

> If a firewall is enabled on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server, you need to check the configured firewall settings. To ensure that events are transmitted, the firewall must be configured to allow transmission through the SSL port that was specified for connecting to the computer with Kaspersky Security Center during installation of the Kaspersky Industrial CyberSecurity for Networks Server.

When the specific types of events are registered in Kaspersky Industrial CyberSecurity for Networks, these events will also be displayed in the Kaspersky Security Center events table.

Types of events 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 types of events in Kaspersky Security Center correspond to the specific types of events 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	Registration as a Kaspersky Security Center incident	Corresponding event type code in Kaspersky Industrial CyberSecurity for Networks
Test event (DPI)	no	4000000001
Test event (NIC)	no	4000000002
Test event (IDS)	no	4000000003
Test event (AM)	no	4000000004
Unauthorized network interaction detected	no	4000002601
System command detected	Only events with the *Critical* severity level	4000002602
No traffic at monitoring point	no	4000002700
TCP protocol anomaly detected: content substitution in overlapping TCP segments	yes	4000002701

Process Control rule violation	Only events with the *Critical* severity level	4000002900
Intrusion Detection rule from the system set of rules was triggered	no	4000003000
Intrusion Detection rule from the custom set of rules was triggered	no	4000003001
Symptoms of ARP spoofing detected in ARP replies	yes	4000004001
Symptoms of ARP spoofing detected in ARP requests	yes	4000004002
New device detected in network	yes	4000005003
New device settings detected	no	4000005004
IP address conflict detected	yes	4000005005
Activity detected from asset with Archived status	no	4000005006
New IP address of device detected	yes	4000005007
New MAC address of device detected	yes	4000005010
IP address added to device	no	4000005009
MAC address added to device	no	4000005008
IP protocol anomaly detected: data conflict when assembling IP packet	yes	4000005100
IP protocol anomaly detected: fragmented IP packet size exceeded	yes	4000005101
IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	yes	4000005102
IP protocol anomaly detected: mis-associated fragments	yes	4000005103
PLC Project Control: detected read of unknown block from PLC	no	4000005200
PLC Project Control: detected read of known block from PLC	no	4000005201
PLC Project Control: detected write of new block to PLC	no	4000005202
PLC Project Control: detected write of known block to PLC	no	4000005203
PLC Project Control: detected read of unknown project from PLC	no	4000005204
PLC Project Control: detected read of known project from PLC	no	4000005205
PLC Project Control: detected write of new project to PLC	no	4000005206
PLC Project Control: detected write of known project to PLC	no	4000005207

Correlation rule event registered	Only events with the *Critical* severity level	8000000000, 8000000001, 8000000002, 8000000003
Maximum number of reported events has been reached	yes	–
User event based on Deep Packet Inspection technology	Only events with the *Critical* severity level	–
User event based on External technology	yes	–

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).

Correspondence between event severities

Kaspersky Security Center event severities	Kaspersky Industrial CyberSecurity for Networks event severity
Informational message	Informational
Warning	Warning
Critical event	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.

Viewing the ICS security state in Kaspersky Security Center

To view the ICS security state in 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.

   Information about the computer status will be displayed in the section for working with the selected object, which appears on the right in the workspace of the selected group.
3. If the section for working with the selected object does not appear, open it by using the right border of the table containing the list of managed devices.

The computer status of the Kaspersky Industrial CyberSecurity for Networks Server corresponds to the ICS security state. The security state of the ICS is determined based on the presence of unprocessed incidents of Kaspersky Security Center. Kaspersky Security Center incidents are registered when certain types of events of Kaspersky Industrial CyberSecurity for Networks are received.

The color of the icon of the Kaspersky Industrial CyberSecurity for Networks Server computer corresponds to one of the following ICS security states:

- Red color: *Critical* status. There are unprocessed incidents of Kaspersky Security Center. This status is displayed if the **Unprocessed incidents detected** condition is enabled for the selected administration group in the list of conditions of the *Critical* status (enabled by default).
- Yellow color: *Warning* status. There are unprocessed incidents of Kaspersky Security Center. This status is displayed if the **Unprocessed incidents detected** condition is enabled for the selected administration group in the list of conditions of the *Warning* status (and if this condition is disabled for the *Critical* status).
- Green color: *OK* status. There are no unprocessed incidents of Kaspersky Security Center.

  > A green icon with the *OK* status may be displayed even if there are unprocessed incidents of Kaspersky Security Center. This is possible if the **Unprocessed incidents detected** condition is disabled for the selected administration group in the lists of conditions for the *Warning* and *Critical* statuses. To correctly display the ICS security state, you must enable the specified condition in the list of conditions for at least one of the *Warning* or *Critical* statuses.

Viewing the ICS security state via SCADA system

To configure 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's 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's Guide*.

Troubleshooting

This section contains a description of possible problems in the operation of Kaspersky Industrial CyberSecurity for Networks and methods for resolving them.

An application component cannot be installed on a selected node

Problem

During installation of the application, 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

Installation of the 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 for component installation. To 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 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

Depending on the method used to connect to the Server, the application informs of operating issues in the following ways:

- When connected through the web interface – the upper part of the application web interface menu displays a red icon next to the 🔔 button.
- When connected through the Application Console – the Console status bar displays a red icon and an error message.

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 section. Root privileges in the operating system are required for providing access to logs.

New application message

Problem

A new application message appeared on the **Application messages** tab in the **Settings** section (when connected to the Server through the web interface).

> 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 **Application messages** tab 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 on the **Application messages** tab. 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.

- *State unknown*, *Malfunction* – if the message just recently appeared, wait 20–30 seconds and check the current state of the application. You can view information about the current state of the application in the Console window.

- *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 section. 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.

To ensure reliable operation of the application:

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.

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 state 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 section on the Deployment tab.

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.

Unknown state of the application

Problem

The Console status bar shows a gray icon and a text message containing a description of a problem (for example, regarding the unknown state of a node that has application components installed).

Solution

This state of Kaspersky Industrial CyberSecurity for Networks signifies that the application was unable to connect to an application component or process.

Wait 20-30 seconds. The application state will change. The following options are available:

- If the problem was not reproduced, the gray icon and message will no longer be displayed in the status bar of the Console.
- If the problem persists, the application will inform of any operating issues.

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 **Load traffic for the event** 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.

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 types of events. You can enable and configure the saving of traffic for relevant types of events.

You cannot enable saving of traffic for event types that are registered as incidents (event type codes: 8000000000, 8000000001, 8000000002 and 8000000003). To save traffic associated with incidents, you need to enable the saving of traffic for the types of events that result in registration of incidents.

Various event types may be used to register incidents. The utilized event types are determined by event correlation rules. However, event correlation rules may be changed when application updates are installed.

You can determine the approximate composition of event types used for incidents by viewing events in previously registered incidents. However, the list of event types obtained in this way will be incomplete. Other types of events may be used in subsequently registered incidents (for example, due to changes in correlation rules after installation of updates). If you want the application to always save traffic for all events within incidents, you can enable the saving of traffic for all system event types (for which it is possible to enable saving of traffic).

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.

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 enabled on the Server and on application sensors. In this case, when viewing information about events and interactions of assets, take into account the time and list of preventive maintenance and adjustment operations to be conducted.
- Disable the 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, to resume control of the protected ICS you need to re-enable the monitoring points 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.

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), make the appropriate changes for Process Control, Network Control, and Asset Management.

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 section. Root privileges in the operating system are required for providing access to logs.

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 a web browser

Problem

When attempting to connect to the Server through a web browser, the Kaspersky Industrial CyberSecurity for Networks web interface page does not load.

Solution

Possible situations:

- There is no network access to the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server with 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 web browser address bar. Enter the Server IP address or computer name that was specified during installation of the Web Server. If the default port 443 is set, you do not have to specify the port number. If a different port number is set, enter the full address `https://<Server name>:<port>` in the address bar.
- JavaScript is disabled in the web browser. A message about this is displayed on the connection failure warning page. In the web 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 web browser displays a certificate warning

Problem

When attempting to connect to the Server, the web browser displays a warning stating that the security certificate or established connection is not trusted. The contents of the warning depend on the specific web browser being used.

Solution

The warning means that a self-signed certificate is being used on the web server. To 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 web browser warning window select the option that lets you continue connecting. After connecting to the Server, the web browser window will display a warning message about the certificate. The text of the message depends on the specific web browser being used.

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 problem in the application documentation or in one of the sources of information about the application, we recommend that you contact Technical Support. Technical Support experts will answer your questions about installing and using the application.

Before contacting Technical Support, please carefully read the technical support rules.

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

- Call Technical Support by phone.
- Submit a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal.

Technical support by phone

In most regions all over the world, you can call Technical Support. You can find information on ways to receive technical support in your region and contact information for Technical Support on the Kaspersky Technical Support website.

Before contacting Technical Support, please carefully read the technical support rules.

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, please 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 section.

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 obtained using the application installation script kics4net-deploy-<application version number>.bundle.sh.

To receive data on application components:

1. On the computer from which the installation was performed, go to the folder containing the saved files from the distribution kit of Kaspersky Industrial CyberSecurity for Networks.
2. Enter the command for running the application installation script with the `gather-artefacts` parameter:

   ```
   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 `SUDO password` invitations, 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.

Sources of information about the application

You can use the following sources to independently find information about Kaspersky Industrial CyberSecurity for Networks:

- Kaspersky Industrial CyberSecurity for Networks page on the Kaspersky website.
- Kaspersky Industrial CyberSecurity for Networks page on the Technical Support website (Knowledge Base).
- Online Help.

If you cannot find a solution to an issue on your own, please contact Kaspersky Technical Support.

An Internet connection is required for accessing information sources on the web.

Kaspersky Industrial CyberSecurity for Networks page on the Kaspersky website

On the Kaspersky Industrial CyberSecurity for Networks page, you can view general information about the application, its functions and features.

Kaspersky Industrial CyberSecurity for Networks page in the Knowledge Base

Knowledge Base is a section on the Technical Support website.

The Kaspersky Industrial CyberSecurity for Networks page in the Knowledge Base provides articles containing useful information and recommendations on application use.

Online Help

Online Help resides on a Kaspersky web resource.

Online Help provides information for performing the following tasks:

- Preparing to install, installing, and uninstalling Kaspersky Industrial CyberSecurity for Networks.
- Configuring and using Kaspersky Industrial CyberSecurity for Networks.
- Interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center.

Online Help also contains information about the common tasks that users can perform with the application depending on the available permissions in Kaspersky Industrial CyberSecurity for Networks.

Online Help includes documentation for the Kaspersky Industrial CyberSecurity for Networks API. This documentation serves as the Developer's Guide for the Kaspersky Industrial CyberSecurity for Networks API. In the Kaspersky Industrial CyberSecurity for Networks API Developer's Guide, you can find information on performing the following tasks:

- Preparing to use Kaspersky Industrial CyberSecurity for Networks API.

- Remotely calling procedures for receiving data from Kaspersky Industrial CyberSecurity for Networks and for sending data to the application.

Appendices

This section provides information that complements the main document text with examples, reference information, and additional data.

Example installation of a Server and sensor

This section describes an example sequence of actions for installing Kaspersky Industrial CyberSecurity for Networks with a Server and one sensor. The computer on which the Server is being installed is referred to as "computer 1" in the example. The computer on which the sensor is being installed is referred to as "computer 2". The installation is performed from computer 1.

To install the Server and sensor on computer 1 and computer 2:

1. On computer 1 and computer 2, set the same password for the root user account (application components will be installed under this user account).

   To set a password, you can enter the `sudo passwd root` command in the command line.

2. On computer 1, create the kics4net_startuser account. This account will be used to run the application installation script. After the application is installed, this account will also be allowed to start the Application Console.

   The kics4net_startuser account does not need to run commands with root privileges. To create the account, you can enter the `sudo useradd kics4net_startuser` command in the command line. After creating the account, you can set a password for it by using the `sudo passwd kics4net_startuser` command.

3. Find out and save the following information about the computers:

   - Name and IP address of computer 1.
   - IP address of computer 2.
   - 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).

4. On computer 1, verify that you can access computer 2 over the SSH protocol.

   To connect:

   a. Enter the following command in the command line:

      ```
      ssh root@<IP address of computer 2>
      ```

   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
      ```

5. On computer 1, sign in to the system using the kics4net_startuser account and create the folder /home/kics4net_startuser/kics4net_install/.

6. Copy the following files from the Kaspersky Industrial CyberSecurity for Networks distribution kit to the folder you created:

   - Application installation script kics4net-deploy-<application version number>.bundle.sh
   - Package for installing the Server and sensors: kics4net-<application version number>.x86_64.rpm
   - Package for installing the Console: kics4net-utm-<application version number>.x86_64.rpm
   - Package for installing the DBMS: kics4net-postgresql-<DBMS version number>.x86_64.rpm
   - Package for installing the Intrusion Detection system: kics4net-suricata-<system version number>.x86_64.rpm
   - Package for installing a web server: kics4net-webserver-<application version number>.x86_64.rpm
   - Package for installing Network Agent from the Kaspersky Security Center distribution kit: klnagent64-<Network Agent version number>.x86_64.rpm

7. Go to the folder /home/kics4net_startuser/kics4net_install/.

8. Enter the command for running the application installation script:

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

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

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

10. After you select the language for the installation menu, the application verifies the checksums of packages in the folder containing the saved files from the distribution kit. Wait for validation of the package checksums to complete.

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

    The main installation menu appears on the screen.

12. Select the **Add Server** menu item and specify the main settings of the Server in the prompts that follow:

    - **Enter the IP address of the node for installation** – type the IP address of computer 1.
    - **Enter the IP address for connections to the Server** – re-enter the IP address of computer 1.
    - **Enter Server name** – type any Server name that is unique in Kaspersky Industrial CyberSecurity (for example, `Server_1`).
    - **Add the capability for application interaction with Kaspersky Security Center** – type `y`, and in the prompts that follow, enter the IP address/name of the computer with Kaspersky Security Center and the SSL port for connection.
    - **Enable time synchronization between Server and sensors** – type `y`.
    - **Enter the IP address or name of the computer with the web server** – type the IP address / name of computer 1.
    - **Enter the web server port number** – type port number 443.
    - **Enter an application user name** – type the application user name `kics4net_admin`.

- **Use self-signed certificates to connect to web server** – type `y` to confirm the use of a self-signed certificate for the Web Server. If you have a certificate that was published by a trusted certificate authority, to use this certificate type `n` at this prompt and then `y` at the prompt to **Use trusted certificates to connect to web server**. To use a trusted certificate, you must specify the path to the trusted certificate file.

  > If you want to use a trusted certificate in the application, it must be issued for the same IP address or computer name that will be indicated by application users when connected through the web interface. To load a trusted certificate, you can use a PFX file containing the saved trusted certificate and private key. The file must be created without a defined password for accessing the contents.

- **Enter the operating system user name for starting the Console** – type the user name `kics4net_startuser`. This user will be allowed to start the Application Console.

- **Specify the name of one more user** – type `n`.

13. Select the **Add sensor** menu item and specify the main settings of the sensor in the prompts that follow:

    - **Enter the IP address of the node for installation** – type the IP address of computer 2.

    - **Enter sensor name** – type any name that is unique for a sensor in Kaspersky Industrial CyberSecurity (for example, `Sensor_1`).

14. Select the **Change interface language** menu item, and select the localization language for components of Kaspersky Industrial CyberSecurity for Networks in the menu that appears.

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

16. When the screen displays a message prompting you to read the terms of the End User License Agreement and Privacy Policy, press **ENTER**.

    The text of the End User License Agreement will appear on the screen.

17. Please carefully read the End User License Agreement.

    After you are finished viewing the End User License Agreement, the screen will display a menu in which you can select your next actions.

18. Select **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.

19. When you see a message about viewing the Privacy Policy, press **ENTER**.

    The text of the Privacy Policy will appear on the screen.

20. Please carefully read the Privacy Policy.

    After you are finished viewing the Privacy Policy, the screen will display a menu in which you can select your next actions.

21. Select **I understand and agree that my data will be processed and transmitted (including to third-party countries) in accordance with the Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.

    After you accept the terms of the Privacy Policy, the screen will prompt you to enter the password of the user running the installation.

22. Enter the root user password. The password must be entered twice: first in the `SSH password` prompt and then in the `SUDO password` prompt.

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

23. When the prompt appears for entering the password of the user kics4net_admin, enter the new password for this user.

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

After installation is complete, Kaspersky Industrial CyberSecurity for Networks does not monitor the industrial network (monitoring points have not been added to network interfaces of nodes that have application components installed). To use the application, you need to perform the necessary actions to prepare the application for operation.

System event types in Kaspersky Industrial CyberSecurity for Networks

Event types are used when registering events in Kaspersky Industrial CyberSecurity for Networks. The list of event types contains the system event types that were automatically created during installation of the application. You can also create additional event types and add them to the list as custom event types.

Each event type corresponds to a specific event registration technology.

System event types based on Deep Packet Inspection technology

This section 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 of event type	Event title	Severity	Registration conditions
4000002900	Process Control rule violation: $ruleName	*Critical*	A Process Control rule configured with this event type was triggered. The following variables are used in the title and description of an event type: • $ruleName – name of the rule. • $tags – received values of tags whose conditions are defined in the rule.
4000000001	Test event (DPI)	*Informational*	A test network packet was detected.

System event types based on Command Control technology

This section 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 of event type	Event title	Severity	Registration conditions
4000002602	$systemCommandShort	Determined by the importance level of the system command	A monitored system command was detected (and no active Network Control rule was created 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.

System event types based on Network Integrity Control technology

This section 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 of event type	Event title	Severity	Registration conditions
4000002601	Unauthorized network interaction detected ($top_level_protocol)	*Warning*	A network interaction that is not specified in an active Network 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 the monitoring point named $monitoringPoint	*Warning*	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)	*Informational*	A test network packet was detected (when Network Integrity Control is enabled).

System event types based on Intrusion Detection technology

This section 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 of event type	Event title	Severity	Registration conditions
4000003000	Rule from the $fileName set (system set of rules) was triggered	Determined based on the rule priority	An Intrusion Detection rule in the system set of rules was triggered (the rule set is in active state). 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. • $severity – priority of the rule.
4000003001	A rule from the $fileName set (custom set of rules) was triggered.	Determined based on the rule priority	An Intrusion Detection rule in the custom set of rules was triggered (the rule set is in active state). 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. • $severity – priority of the rule.
4000004001	Symptoms of ARP spoofing detected in ARP replies	*Critical*	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	*Critical*	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	*Critical*	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	*Critical*	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	*Critical*	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	*Warning*	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	*Critical*	TCP protocol anomaly detected: packets contain overlapping TCP segments with varying contents.
4000000003	Test event (IDS)	*Informational*	A test network packet was detected (with rule-based Intrusion Detection enabled).

System event types based on Asset Management technology

This section 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 of event type	Event title	Severity	Registration conditions
4000005003	Detected new asset with the address	*Critical*	Asset Management monitoring mode resulted in the automatic addition of a new asset based

	$owner_ip_or_mac		on a detected IP address or MAC address that has not been specified for other assets in the table. The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the asset. • $asset_name – assigned name of the asset. • $assigned_mac – assigned MAC address (if defined). • $owner_ip – assigned IP address (if defined). • $asset_id – ID of the asset.
4000005004	Received new information about asset with the address $owner_ip_or_mac	*Informational*	Asset Management monitoring mode resulted in the automatic update of asset 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 asset. • $asset_name – name of the asset. • $updated_params – list of updated information. • $asset_id – ID of the asset.
4000005005	IP address $owner_ip conflict detected	*Critical*	In Asset Management monitoring mode, the application detected the use of an IP address by a different asset than the asset 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 asset that used the IP address. • $challenger_mac – MAC address of the asset that used the IP address. • $asset_name – name of the asset in whose settings the IP address was specified. • $owner_mac – MAC address of the asset in whose settings the IP address was specified.

			• $challenger_ips_list – list of other IP addresses of the asset that used the IP address. • $asset_id – ID of the asset in whose settings the IP address was specified. • $challenger_id – ID of the asset that used the IP address.
4000005006	Detected traffic from address $owner_ip_or_mac, which is assigned to an asset with the Archived status	*Critical*	In Asset Management monitoring mode, activity was detected from an asset that was assigned the *Archived* status. The following variables are used in the title and description of an event type: • $owner_ip_or_mac – IP or MAC address of the asset. • $asset_name – name of the asset. • $last_seen_timestamp – date and time when the asset was last seen in the network. • $asset_id – ID of the asset.
4000005007	A new IP address $new_ip_addr was detected for the asset with MAC address $owner_mac	*Critical*	In Asset Management monitoring mode, a new IP address used by an asset 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 asset. • $asset_name – name of the asset. • $owner_ips_list – list of other IP addresses of the asset. • $asset_id – ID of the asset.
4000005008	MAC address $owner_mac was added to the asset with IP address $owner_ip	*Informational*	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 asset 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 asset. • $owner_ip – IP address of the asset.

			• $asset_name – name of the asset. • $asset_id – ID of the asset.
4000005009	IP address $owner_ip was added to the asset with MAC address $owner_mac	*Informational*	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 asset 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 asset. • $owner_mac – MAC address of the asset. • $asset_name – name of the asset. • $asset_id – ID of the asset.
4000005010	Detected new MAC address $new_mac_addr for asset with the IP address $owner_ip	*Critical*	Asset Management monitoring mode resulted in the detection of a new MAC address used by an asset (autoupdate of address information is disabled for the asset). 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 asset • $asset_name – name of the asset. • $asset_id – ID of the asset.
4000005200	PLC Project Control: detected read of unknown block from PLC $asset_name	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $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	*Critical*	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).

			The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $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	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $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	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $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	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $saved_date_time – date and time when the operation was detected.
4000005205	PLC Project Control: detected read of known project from PLC $asset_name	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $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	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $saved_date_time – date and time when th.e operation was detected.
4000005207	PLC Project Control: detected write of known project to PLC $asset_name	*Critical*	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). The following variables are used in the title and description of an event type: • $asset_name – name of the asset. • $saved_date_time – date and time when the project was saved in the application.
4000000004	Test event (AM)	*Informational*	A test network packet was detected (with the asset activity detection method enabled).

System event types based on External technology

This section provides a description of system event types associated with External technology (see the table below).

System event types based on External technology (EXT)

Code of event type	Event title	Severity	Registration conditions
8000000000	Incident	Determined by the importance level of the correlation rule	A sequence of events that satisfy the conditions of a correlation rule was detected (if the incident title and description are not defined in the rule).
8000000001	$customTitle	Determined by the	A sequence of events that satisfy the conditions of a

		importance level of the correlation rule	correlation rule was detected (if an incident title is defined in the rule but not an incident description). The event type title uses the $customTitle variable, which is replaced with the incident title when an event is registered.
8000000002	Incident	Determined by the importance level of the correlation rule	A sequence of events that satisfy the conditions of a correlation rule was detected (if an incident description is defined in the rule but not an incident title). The event type description uses the $customDescription variable, which is replaced with the incident description when an event is registered.
8000000003	$customTitle	Determined by the importance level of the correlation rule	A sequence of events that satisfy the conditions of a correlation rule was detected (if the incident title and description are defined in the rule). The following variables are used in the title and description of an event type: • $customTitle – title of the incident. • $customDescription – description of the incident.

Files for importing custom tags and device configurations

You can import descriptions of custom tags and device configurations into Kaspersky Industrial CyberSecurity for Networks. The import is performed 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). This section describes the common structures of data files.

The following set of data files is required for importing tags and devices into Kaspersky Industrial CyberSecurity for Networks:

- devices.csv. Contains descriptions of devices and 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.

- connections.csv. Contains descriptions of connection 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.

- iec61850_sv_messages.csv. Contains descriptions of messages for the IEC 61850: Sampled Values protocol.

When using data files, consider the following specifics:

- Data files must have UTF-8 encoding.
- All data files must be located in the same folder.
- 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. Note that the enums.csv and datasets.csv files must be located in the import folder.

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. A connection ID specified in the device description file is used in the connections and protocols description file for purposes of linking with tags and protocols.

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 AFV series
- 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

- `Connection` is the connection ID from the connections.csv file containing a description of connections and protocols.

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"
```

File with descriptions of connections and protocols: connections.csv

The protocol description file contains descriptions of protocols for each connection.

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.
- `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 – EMERSON CONTROLWAVE DATA EXCHANGE
    - 27 – HONEYWELL CONTROLEDGE 900 INTERACTION

- `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 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 f
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=S
  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"`

- EMERSON CONTROLWAVE DATA EXCHANGE:

  `"IP-Address=192.168.0.7;Port=1234"`

- HONEYWELL CONTROLEDGE 900 INTERACTION:

  `"IP-Address=192.168.1.99;Port=41103"`

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;EngUnit
```

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.

- `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 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 file enums.csv, 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;EngUnit
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
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.

- EMERSON CONTROLWAVE DATA EXCHANGE: a 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.

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. 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";"Unbuffer
```

File with descriptions of Sampled Values protocol messages: iec61850_sv_messages.csv

The file with descriptions of Sampled Values protocol messages contains the parameters for messages of the IEC 61850: Sampled Values protocol.

The file should begin with header strings containing the data needed for file processing. An example of header strings of the iec61850_sv_messages.csv file is provided below.

```
Example:
'SVMessages
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalF
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalFiel` contains the names of columns containing data:

- `Connection` – ID of the connection associated with the string of settings in the file iec61850_sv_messages.csv.

- `SVControlBlockName` – name of the control block for this message.

- `SampledValuesId` – message ID.

- `ConfRev` – configuration revision.

- `DataSetName` – name of the data set associated with this message.

- `IsMulticast` – type of transmission. Takes the `Multicast` or `Unicast` value.

- `OptionalFields` – list of additional (optional) fields included in the message body for transmission.

The header strings are followed by the file body containing the parameter values (connection ID, control block name, message ID, configuration revision, name of the data set for the message, type of transmission, and additional fields). An example of the iec61850_sv_messages.csv file is provided below.

Example:

```
'SVMessages
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;SVControlBlockName;SampledValuesId;ConfRev;DataSetName;IsMulticast;OptionalF
"IED_TRANSFORMER1";"IED_TRANSFORMER1/LLN0$MS$SMV_Control_Block1";"SMV_ID_1";"0";"IED_TRA
```

Glossary

ARP spoofing

A technique used by criminals to conduct a "man-in-the-middle" attack on networks that use ARP (Address Resolution Protocol).

SCADA

Abbreviation for Supervisory Control And Data Acquisition. A software suite that enables the operator to control industrial processes in real time.

SIEM

Abbreviation for Security Information and Event Management. This is a solution for managing information and events in an organization's security system.

ICS

Abbreviation for Industrial Control System. A package of hardware and software designed to automate control of process equipment at industrial enterprises.

Kaspersky Industrial CyberSecurity for Networks Web Server

Kaspersky Industrial CyberSecurity for Networks component. Provides an interface for connecting to the Kaspersky Industrial CyberSecurity for Networks Server through a web browser.

External

Technology for registering incidents as well as events that are received by Kaspersky Industrial CyberSecurity for Networks from external systems using Kaspersky Industrial CyberSecurity for Networks API methods.

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.

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.

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.

Network map

A model that visually represents detected communications between industrial network devices. The network map contains the following objects: nodes representing assets, asset groups, and links between nodes/asset groups.

Kaspersky Industrial CyberSecurity for Networks Console

Kaspersky Industrial CyberSecurity for Networks component. It provides a graphical user interface for connecting to the Server, and lets you configure functionality that cannot be managed when connected through a web browser.

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).

Deep Packet Inspection

Technology for registering events associated with process violations (for example, the set temperature value has been exceeded).

Asset management

Technology for registering events associated with the detection of activity of devices in traffic (for example, detection of activity shown by a previously unknown device).

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 a prohibited protocol).

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).

Security policy

Set of data that defines the process control settings and the settings for registering different types of events.

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.

Network Control rule

A description of authorized communications for industrial network devices. When Kaspersky Industrial CyberSecurity for Networks detects network interaction that satisfies an active network control rule, it does not register an event.

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.

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.

Programmable Logic Controller (PLC)

Industrial controller used to automate enterprise processes.

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.

Industrial network

Computing network that links the nodes of an automated Industrial Control System of an industrial enterprise.

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.

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 a copy of industrial network traffic from monitoring points, processes the obtained data and relays it to the Server.

Kaspersky Industrial CyberSecurity for Networks Server

Kaspersky Industrial CyberSecurity for Networks component. The Server processes industrial network traffic information, saves this information, and provides the necessary data (for example, events and asset information). The Server can receive industrial network traffic information from the monitoring points on sensors or from its own monitoring points.

System command

Data block in industrial network traffic containing the device management command (for example, START PLC) or system message related to device operation (for example, REQUEST NOT FOUND).

Event

A record containing information about the detection of data requiring the attention of an ICS security officer in industrial network traffic. 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.

Link on the network map

Object on the network map depicting interaction between nodes represented by a line between those nodes.

Tag

Variable that contains the value of a specific process parameter such as temperature.

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. Kaspersky Industrial CyberSecurity for Networks uses system event types and custom event types. System event types are created by the application during installation and cannot be deleted. Custom event types can be manually created, edited, and deleted.

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).

Notification

A message with information about an event (or events), which is sent by the application via notification delivery systems (for example, via email) to the specified addresses.

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 assets.

Device

An industrial network device used to automate an industrial process at an enterprise (for example, a programmable logic controller, remote terminal, or intelligent electronic device).

AO Kaspersky Lab

Kaspersky is an internationally renowned vendor of systems for computer protection against various types of threats, including viruses, malware, spam, network and hacker attacks.

In 2008, Kaspersky was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky is the preferred vendor of computer protection systems for home users in Russia ("IDC Endpoint Tracker 2014").

Kaspersky was founded in 1997 in Russia. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3000 highly qualified specialists.

Products. Kaspersky products protect both home computers and corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with the centralized management tools of Kaspersky, these solutions ensure effective automated protection against computer threats for organizations of any scale. Kaspersky products are certified by major testing laboratories, compatible with the applications of most software vendors, and optimized for work on most hardware platforms.

Virus analysts work around the clock at Kaspersky. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include the signatures of these threats in the databases used by Kaspersky applications.

Technologies. Many of technologies that make part of any modern anti-virus were first developed by Kaspersky. It is therefore logical for many third-party software developers to use the kernel of Kaspersky Anti-Virus in their own applications. Those companies include Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Many of the company's innovative technologies are backed by patents.

Achievements. Years of struggle against computer threats have brought hundreds of awards to Kaspersky. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. However, the most important award to Kaspersky is the commitment of users all over the world. The company's products and technologies protect more than 400 million users. The number of its client organizations exceeds 270 thousand.

Kaspersky website:	https://www.kaspersky.com
Virus Encyclopedia:	https://securelist.com/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com/ (for scanning suspicious files and websites)
Kaspersky user community:	https://community.kaspersky.com

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Flash is either a registered trademark or trademark of Adobe Systems Incorporated in the United States and/or other countries.

Antaira is a registered trademark of Antaira Technologies, LLC.

Apple, iPad, iPhone, Mac, macOS, Mac OS, and OS X are trademarks of Apple Inc., registered in the United States and other countries.

AXIS and AXIS COMMUNICATIONS are registered trademarks or trademark applications of Axis AB in various jurisdictions.

BitTorrent is a trademark of BitTorrent, Inc.

Cisco and IOS are trademarks of Cisco Systems, Inc. and/or its affiliates registered in the United States and elsewhere.

Dell is a trademark of Dell, Inc. or its subsidiaries.

Radmin is a registered trademark of Famatech.

FreeBSD is a registered trademark of The FreeBSD Foundation.

General Electric and MULTILIN are registered trademarks of General Electric Company.

Android, Google, and Google Chrome are trademarks of Google, Inc.

Intel and Core are trademarks of Intel Corporation registered in the United States and elsewhere.

IBM and DB2 are trademarks of International Business Machines Corporation, registered in many jurisdictions.

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

Microsoft, SQL Server, Windows, Windows Server, and Windows Vista are registered trademarks of Microsoft Corporation in the United States and elsewhere.

MOXA is a registered trademark of Moxa Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

IPX is a registered trademark of Novell Inc. in the United States and other countries.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

Pilz is a registered trademark of Pilz GmbH & Co. KG.

Python is a trademark or registered trademark of Python Software Foundation.

Realtek is a trademark of Realtek Semiconductor Corporation.

CentOS is a trademark of Red Hat, Inc.

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.

Dameware is a trademark of SolarWinds Worldwide, LLC registered in the United States and elsewhere.

Texas Instruments is a trademark of Texas Instruments.

Tor is a trademark of The Tor Project registered in the United States (U.S. Registration № 3 465 432).

SecureCRT is a trademark of VanDyke Software, Inc.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.