kaspersky

Kaspersky Industrial CyberSecurity for Networks

© 2026 AO Kaspersky Lab

Contents

About Kaspersky Industrial CyberSecurity for Networks
- Distribution kit
- Hardware and software requirements
- Security recommendations for Kaspersky Industrial CyberSecurity for Networks

What's new

Overview of Kaspersky Industrial CyberSecurity for Networks functionality
- Asset Discovery
- Advanced Asset Management
- Security audit
- Threat and Anomaly Detection
- Extended Threat Detection and Response
- Ecosystem and Integrations

Application architecture

Common deployment scenarios
- Installing a Server without external sensors
- Installing a Server and external sensors
- Connecting Kaspersky Industrial CyberSecurity for Networks to an industrial network via data diodes
- Receiving industrial network traffic from Kaspersky SD-WAN components

Getting started: basic scenario

Installing and removing the application
- Ports used for installation and operation of components
- Centralized installation and removal of application components
  - Requirements for centralized installation of application components
  - Preparing for centralized installation of components
  - Centralized installation of application components
  - Centralized installation of application components in non-interactive mode
  - Centralized installation menu commands
  - Reconfiguration and centralized reinstallation of application components
  - Centralized removal of application components
- Local installation and removal of application components
  - Requirements for local installation of application components
  - Preparing for local installation of the Server or a sensor
  - Using a script for local installation of application components
  - Using a script for local removal of application components
- Reinforcing the security of computers with application components installed
- Configuring a firewall on Server and sensor nodes
- Installing the Kaspersky Industrial CyberSecurity for Networks Administration Plug-in for Kaspersky Security Center
- Startup configuration of the application after Server installation
- Certificates used in Kaspersky Industrial CyberSecurity for Networks
  - Updating the main certificate of the Kaspersky Industrial CyberSecurity for Networks Server
  - Updating the certificate for connecting to the Server through the web interface
  - Updating the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API

Updating certificates for connecting connectors
Updating certificates for connections with the Endpoint Agent software components
Updating using data migration script
Installing an updated application version with a patch
Starting and stopping the application
Connecting to the Server through the web interface
Terminating a Server connection session through the web interface
Connecting to a sensor through the web interface
Application interface
About the Kaspersky Industrial CyberSecurity for Networks Server web interface
About the Kaspersky Industrial CyberSecurity for Networks sensor web interface
Server web interface menu during startup configuration of the application
Server web interface menu during normal operation of the application
Initial configuration section
Dashboard section
Assets section
Network map section
Events section
Reports section
Process control section
Allow rules section
Detection rules section
Risks section
Security audit section
Settings section
Licensing the application
About the End User License Agreement
About the Privacy Policy
About the license
About the license certificate
About the license key
About the license key file
Adding a license key when connected to the Server through the web interface
Viewing information about an added license key
Removing a license key
Data provision
Folders for storing application data
About logs
Administration of Kaspersky Industrial CyberSecurity for Networks
Deploying nodes
Adding and deleting sensors
Adding and connecting a sensor using the sensor web interface
Using a communication data package to add and connect a sensor
Adding and connecting a sensor automatically over the network
Creating a new communication data package for a sensor
Removing a sensor

- Changing the main node settings
  - Changing the application data storage settings on a node
  - Renaming a node that has application components installed
  - Connecting and configuring external storage for traffic dump files
- Managing monitoring points 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
- Managing technologies
  - Enabling and disabling technologies
  - Configuring technology operating modes
  - Managing inheritance of technologies
- Downloading traffic received by the node monitoring points

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
- Viewing information about nodes with application components installed and about network interfaces on nodes
  - Node information displayed in the details
  - Network interface information displayed in the details
- 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
- Checking the integrity of application modules
- Synchronizing the time on nodes of Kaspersky Industrial CyberSecurity for Networks with the time source used for industrial network devices

Updating databases and application modules

- Manually starting an update
- Configuring automatic updates
- Viewing information about update installation
- Restarting services on the nodes after installing the OpenSSL library update

Distributing access to application functions

- About application user accounts
- Application functions that are available when connected to the Server through the web interface
- Viewing information about application user accounts
- Creating an application user account
- Changing the role of an application user account
- Administrator-initiated password change
- Managing user lockout
- Deleting an application user account

Configuring Asset Management

- Asset Management methods and modes
- Selecting sources of vulnerability data

- Manually adding devices
  - Adding a device when working with the table of devices
  - Adding a device when working with the topology map
  - Adding a device based on the node of an unknown device on the network interaction map
  - Adding a device based on an unmanaged switch on the topology map
- Merging devices
  - Merging devices when working with the table of devices
  - Merging devices when working with the networking interactions map and the topology map
- Deleting devices
  - Deleting devices when working with the table of devices
  - Removing devices when working with the networking interactions map and the topology map
- Manually changing the statuses of devices
  - Changing the statuses of devices when working with the table of devices
  - Changing the statuses of devices when working with the networking interactions map and the topology map
- About arranging devices into groups
- Automatic grouping of devices based on a specific criterion
  - Automatically grouping devices based on a specific criterion beginning with the top level of the hierarchy in the group tree
  - Automatically grouping devices in a selected device group:
- Manually arranging devices into groups
  - Add one device to a group
  - Add multiple devices to a group
  - Remove one device from a group
  - Remove multiple devices from groups
- Moving nodes and groups to other groups on the network interaction map
- Manually creating a device group tree
  - Add group
  - Rename group
  - Deleting groups
  - Move group
  - Search groups
  - Update the tree
- Adding and removing labels for devices
  - Adding labels for one device
  - Adding labels for multiple devices
  - Removing labels from one device
  - Clearing lists of labels for multiple devices
- Editing device information
- Adding, editing and deleting custom fields for a device
- Deleting device users
- Removing device executable files

Configuring address spaces

- About address space rules
- About address space subnets
- Adding an address space

- Generating a list of subnets for asset management
  - Adding a subnet
  - Editing subnet settings
  - Deleting subnets
- Viewing information about devices with IP addresses from the selected subnets
- Changing an address space
- Deleting an address space

Configuring Process Control
- Supported devices and protocols
- Process Control devices
  - Process Control settings for devices
  - About automatic detection of Process Control settings for devices
  - Manually adding Process Control settings for a device
  - Editing Process Control settings for a device
  - Selecting the monitored system commands
  - Clearing Process Control settings defined for a device
  - Importing configurations of devices and tags from external projects
  - Supported types of projects for importing
- Tags
  - About Unknown Tag Detection
  - Manually adding a tag
  - Editing tag parameters
  - Adding tags to the favorites list
  - Deleting tags
- Process Control rules
  - Rules with defined conditions for tag values
  - Rules with Lua scripts
  - Process Control rules learning mode
  - Viewing the table of Process Control rules
  - Creating a Process Control rule with settings of conditions
  - Creating a Process Control rule with a Lua script
  - Editing Process Control rule settings
  - Creating, viewing and editing a global Lua script
  - Deleting Process Control rules

Configuring Interaction Control
- Learning mode for Interaction Control technologies
- Monitoring mode for Interaction Control technologies
- Automatic generation of Interaction Control rules in learning mode
- Automatic generation of Interaction Control rules when importing configurations from external projects
- Viewing Interaction Control rules in the table of allow rules
- Fine-tuning Interaction Control for individual devices
- Manually creating Interaction Control rules
  - Creating an interaction control rule with blank settings or settings from a template
  - Creating an interaction control rule from an existing one
  - Creating a rule based on an event registered for Network Integrity Control or Command Control technology
- Editing Interaction Control rule settings
- Enabling and disabling Interaction Control rules

- Suspending and resuming monitoring of the network interactions of devices
- Deleting Interaction Control rules

Configuring Intrusion Detection and Network Anomaly Detection

- Managing Intrusion Detection rule sets
  - Enabling and disabling sets of Intrusion Detection rules
  - Loading and replacing user-defined sets of Intrusion Detection rules
  - Removing user-defined sets of Intrusion Detection rules
- Using additional Intrusion Detection methods
- Managing Network Anomaly Detection rules
  - Creating Network Anomaly Detection rule
  - Changing Network Anomaly Detection rule
  - Generating SQL query texts for Network Anomaly Detection rules
  - Viewing the table of Network Anomaly Detection rules:
  - Enabling and disabling network anomaly detection rules
  - Manually starting and stopping a Network Anomaly Detection rule
  - Viewing general information about triggers for network anomaly detection rules
  - Deleting Network Anomaly Detection rules
- Managing dictionaries for Network Anomaly Detection rules
  - Adding a dictionary
  - Viewing a dictionary table
  - Editing dictionary settings
  - Deleting dictionaries

Managing logs

- Managing the settings for storing logs in the Server database
- Managing the settings for saving traffic in the Server database
- Managing the settings for saving traffic dump files
- Enabling and disabling the user activity audit
- Changing the logging level for processes

Configuring operation with EPP applications

- Scenario for preparing to receive data from EPP applications
- Adding an integration server
- Creating a communication data package for integration server clients
- Integration servers table
- Enabling and disabling an integration server in the necessary mode
- Editing integration server settings
- Removing an integration server

Managing response actions in Kaspersky Industrial CyberSecurity for Networks

- Triggering event response actions
- Triggering response actions when working with device executable files
- Triggering device response actions
- Triggering response actions when working with registered response actions
- Viewing the response action table
- Downloading files containing data from the standard output and error streams when starting a process
- Deleting response actions

Managing connectors

- About manageable and unmanageable connectors
- About forwarding events, application messages and audit entries to recipient systems

- Automatic network access control for devices via Cisco Switch connectors
- Adding a connector
- Viewing the connectors table
- Enabling and disabling a connector
- Editing connector settings
- Creating a new communication data package for a connector
- Deleting a connector
- Adding and deleting connector types
  - Viewing the connector types table
  - Adding a connector type
  - Deleting a connector type

Managing security audit jobs

- Vulnerability and compliance audit jobs
  - Adding a vulnerability and compliance audit job
  - Editing a vulnerability and compliance audit job
  - Viewing the table of vulnerability and compliance audit jobs
  - Manually starting and stopping vulnerability and compliance audit jobs
  - Viewing general information about the vulnerability and compliance audit job runs
  - Stopping a device scan in a vulnerability and compliance audit job
  - Deleting vulnerability and compliance audit jobs
  - Managing storage settings for the runs of vulnerability and compliance audit jobs
- Configuration control jobs
  - Adding a configuration control job
  - Editing a configuration control job
  - Viewing the table of configuration control jobs
  - Manually starting and stopping configuration control jobs
  - Viewing general information about the configuration control job runs
  - Assigning a golden device configuration
  - Stopping a device scan in a configuration control job
  - Deleting configuration control jobs
- Active device polling jobs
  - Adding active polling job
  - Editing an active polling job
  - Viewing the table of active polling jobs
  - Starting and stopping active polling jobs
  - Viewing general information about the active polling job runs
  - Viewing a report on the active polling job execution
  - Deleting active polling jobs

Forming a topology map

- Nodes on the topology map
- Links on the topology map
- Viewing details about objects on the topology map
- Adding nodes to the topology map
- Manually adding links to the topology map
  - Adding links for a selected node and configuring additional topology settings
  - Adding links for selected nodes without configuring additional topology settings
- Editing the topology settings for a node

- Renaming the node of an unmanaged switch
- Deleting objects from the topology map
- Changing the topology map scale
- Positioning of the topology map
- Pinning and unpinning nodes on the topology map
- Manually changing the location of nodes on the topology map
- Automatically arranging nodes on the topology map
- Filtering objects on the topology map
- Saving and loading topology map display settings
  - Adding a new view while saving the current topology map display settings
  - Updating a view while saving the current topology map display settings
  - Renaming a topology map view
  - Deleting a topology map view
  - Applying saved view settings on the topology map
- Search for nodes on the topology map

Configuring event types
- Viewing the table of event types
- Editing the settings of a system event type
- Configuring automatic saving of traffic for system event types
- Configuring forwarding of events via connectors
- Common variables for substituting values in Kaspersky Industrial CyberSecurity for Networks

Configuring risk types
- Viewing the table of risk types
- Changing the base score for a risk type
- Managing the settings for storing risks

Managing sets of rules for vulnerability and compliance audit jobs
- Vulnerability and compliance audit rules
- Viewing the table of vulnerability and compliance audit rule sets
- Importing vulnerability and compliance audit rule sets
- Changing vulnerability and compliance audit rule sets
- Deleting vulnerability and compliance audit rule sets

Managing account credentials secrets for remote connections
- Adding a secret
- Viewing the secret table
- Protecting against compromise of secrets when connected to remote devices
- Changing the settings of a secret
- Deleting secrets

Managing reports and report templates
- Duplicating a report template
- Editing a report template
- Deleting a report template
- Deleting a report
- Canceling report generation
- Managing the settings for storing report files

Managing a security policy
- Exporting a security policy in the Server web interface
- Exporting a security policy using the export utility

- Importing a security policy from a file
- Clearing the current security policy
- Converting a security policy from a previous version of the application

Using the Kaspersky Industrial CyberSecurity for Networks API

- Securing interactions when using the Kaspersky Industrial CyberSecurity for Networks API
- Creating and using connectors for the Kaspersky Industrial CyberSecurity for Networks API
- Subscribing to notifications about tag values over the WebSocket protocol

Performing common tasks

- System monitoring in online mode
  - Adding a widget
  - Configuring how widgets are displayed
    - Moving a widget
    - Changing the size of a widget
    - Changing the settings for displaying data in a widget
  - Information in the Devices widget
  - Information in the Events widget
  - Conditions determining how devices are taken into account in the Protection by EPP applications widget
  - Removing a widget
- Asset Management
  - Table of devices
  - Viewing device information
  - Automatically adding and updating devices
  - Automatically merging devices
  - Automatically assigning the statuses of devices
  - Device group tree
  - Monitoring the network behavior of devices
  - Resetting deviations in the network behavior of devices
  - Monitoring read and write of PLC projects
  - Monitoring OT devices equipment
  - Monitoring Windows and Linux device equipment
  - Monitoring device users
  - Monitoring device applications and patches
  - Launch control of executable files on devices
  - Device configuration control
  - Comparison of saved device configurations
- Working with the network interaction map
  - Nodes on the network interaction map
  - Groups of devices on the network interaction map
  - Links on the network interaction map
  - Viewing details about objects
  - Changing the scale of the network interaction map
  - Positioning the network interaction map
  - Pinning and unpinning nodes and groups
  - Manually changing the location of nodes and groups
  - Automatic arrangement of nodes and groups
  - Searching for nodes on the network map

- Filtering objects on the network interaction map
  - Comprehensive filtering of nodes and links
    - Filtering using a period on the time scale
    - Filtering by registered events
  - Filtering of nodes
    - Filtering nodes by device status
    - Filtering nodes by device security state
    - Filtering nodes by device category
    - Enabling and disabling the display of nodes associated with filtered nodes
  - Filtering links
    - Filtering links by criticality score
    - Filtering links by communication protocol
    - Filtering links by OSI model layer
  - Resetting the filter settings
- Saving and loading network interaction map display settings
  - Adding a new view while saving the current network interaction map display settings
  - Updating a view while saving the current network interaction map display settings
  - Renaming a network interaction map view
  - Deleting a network interaction map view
  - Applying saved view settings on the network interaction map
- Downloading traffic when working with the network interaction map

Network session monitoring
- Network sessions table
- Viewing network session details
- Downloading network session traffic

Monitoring events and incidents
- Scores and severities of events
- Event registration technologies
- Event statuses
- Table of registered events
- Viewing events included in an incident
- Viewing event details
- Changing the statuses of events
- Viewing details of EDR incidents
- Creating allow rules for events
  - Creating an allow rule with blank settings or settings from a template
  - Creating an allow rule from an existing one
  - Creating an allow rule from a registered event
- Setting markers
- Copying events to a text editor
- Loading traffic for events
- Exporting activity event data into a file of indicators of compromise
- Creating a folder for exporting events to a network resource

Monitoring risks
- About risks in the Vulnerability category
- Scenario for implementing the continuous risk management process
- Viewing the risks table

- Viewing risk details
- Manually changing the statuses of risks
- Viewing risk details when working with the table of devices
- Deep Packet Inspection
- Monitoring process parameter values
- Settings of tags
- Viewing the table of tags
- Detecting default passwords when connecting to devices
- Obtaining reports
- Viewing the reports table
- Exporting a report to a file
- Reports based on templates
- Viewing the report templates table
- Viewing report template details
- Generating a report based on a template manually
- Reports on vulnerability and compliance audit jobs
- Generating a report on a manual job run
- Generating a report on a manual device scan
- Detecting security issues in encryption protocols
- Typical actions when working with data tables
- Viewing a data table
- Configuring the columns display and order
- Filtering based on standard time periods
- Filtering based on a specified time period
- Filtering by columns
- Table search
- Resetting the defined filter and search settings
- Table sorting
- Selecting elements in a data table
- Navigating to related items in other web interface sections
- Exporting data from a table to a file
- Updating a data table
- Changing your account password
- Managing the application through Kaspersky Security Center
- Enabling and configuring interaction with Kaspersky Security Center
- Adding a license key to Kaspersky Industrial CyberSecurity for Networks from Kaspersky Security Center
- Receiving updates from the Kaspersky Security Center Administration Server
- Monitoring events via Kaspersky Security Center
- Event types 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
- Connecting to the Server computer from Kaspersky Security Center
- Centrally monitoring systems with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console
- About updating the Kaspersky Industrial CyberSecurity for Networks administration web plug-in
- Scenario for Single Sign-On (SSO) technology usage preparations

Granting Kaspersky Security Center users the access rights corresponding to their user roles in Kaspersky Industrial CyberSecurity for Networks
Widgets for monitoring systems and Kaspersky Industrial CyberSecurity for Networks Servers
Widget for Statuses in KICS for Networks
Widget for Critical events in KICS for Networks
Widget for Devices with issues in KICS for Networks
Widget for Up-to-date events of KICS for Networks
Widget for KICS for Networks deployment map
Widget for Information about KICS for Networks Servers
Searching devices and events in the databases of Kaspersky Industrial CyberSecurity for Networks Servers
Configuring the device search settings
Configuring the event search settings
Viewing the search results table
Mapping components of Kaspersky Industrial CyberSecurity for Networks
Generating a list of sites for the main map
Adding a site
Renaming a site
Deleting a site
Changing the background image of a map
Generating lists of Servers within sites
Adding a Server to a site
Removing a Server from a site
Managing the arrangement of objects on maps
Muting a Server in the Web Console
Viewing information about Servers on maps
Troubleshooting
An application component cannot be installed on a selected node
Application problems detected
New application message
Not enough free space on hard drive
An error occurs when enabling a monitoring point
No traffic at monitoring point
Traffic is not being loaded for events or incidents
Preventative maintenance and adjustment operations on the ICS
Unexpected system restart
Connector and remote connection functionality is unavailable after changing or adding the Server IP address
Updates from the Kaspersky Security Center Administration Server are not received
After the Kaspersky Security Center Administration Server is reinstalled, Network Agent cannot be synchronized
Unable to connect to the Server through the web interface
When connecting to the Server, the browser displays a certificate warning
Contacting Technical Support
How to get technical support
Technical Support via Kaspersky CompanyAccount
Collecting information for Technical Support
Sources of information about the application

Appendices
Installing and configuring the CentOS Stream 9 operating system
Configuring time synchronization via the NTP and PTP protocols
Configuring time synchronization via the NTP protocol in CentOS
Configuring time synchronization via the PTP protocol in CentOS
Supported ASDU types identification in protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards
Loading, processing, and managing device and tag configurations with support for IEC 61850 standard protocols
Sending Kaspersky Industrial CyberSecurity for Networks events to SIEM systems
Verifying event forwarding using an HP ArcSight system (as an example)
Format of messages forwarded to a SIEM system
Changing Kaspersky Industrial CyberSecurity for Networks configuration settings using a script
Specifics of connecting Kaspersky Industrial CyberSecurity for Networks nodes as connection gateways in Kaspersky Security Center
Files for importing a universal project
File with descriptions of devices: devices.csv
Connections description file: 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
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 Asset Management technology
System event types based on Network Integrity Control technology
System event types based on Intrusion Detection technology
System event types based on External technology
System event types based on Endpoint Protection Platform
Categories of system commands in Kaspersky Industrial CyberSecurity for Networks
Examples of using address spaces in Kaspersky Industrial CyberSecurity for Networks
Supported common protocols
Details on retrieving configurations for device types using configuration control jobs
Configurations of devices running Windows operating systems
Configurations of devices running Linux operating systems
Configurations of devices categorized as network equipment
Configurations of PLCs and other devices received using Active poll connectors
Commands used for scanning Linux devices in security audit jobs.
Device operating systems supported to perform active polling of devices
Detecting attributes and typical device interactions in Kaspersky Industrial CyberSecurity for Networks
Configuring port mirroring for Kaspersky Industrial CyberSecurity for Networks
Configuring port mirroring for Cisco Access and Distribution switches
Configuring port mirroring for Cisco Small Business™ switches
Configuring port mirroring for Hirschmann industrial Ethernet switches
Configuring port mirroring for Siemens SCALANCE switches
Configuring port mirroring for Siemens RUGGEDCOM i800, i801, i802, i803 switches

Glossary
- Account role
- Address space (AS)
- ARP spoofing
- Asset Management
- Command Control
- CVE
- Dedicated Kaspersky Industrial CyberSecurity network
- Deep Packet Inspection
- Device
- Device vulnerability
- Endpoint Protection Platform
- Endpoint Protection Platform (EPP)
- EPP application
- Event
- Event correlation rule
- Event type
- External
- ICS
- Incident
- Industrial network
- Intelligent electronic device (IED)
- Interaction Control rule
- Intrusion Detection
- Intrusion Detection rule
- IOC
- IOC file
- Kaspersky Industrial CyberSecurity for Networks Sensor
- Kaspersky Industrial CyberSecurity for Networks Server
- Link on the network map
- Manageable connector
- Monitoring point
- Network Anomaly Detection rule
- Network behavior deviations
- Network Integrity Control
- Network interaction map
- Node
- PLC project
- Process Control rule
- Programmable Logic Controller (PLC)
- Risk
- Risk type
- SCADA
- Security policy
- SIEM
- Single Sign-On (SSO) technology
- System command

Tag
Topology Map
Unmanaged connector
Unmanaged switch
Information about third-party code
Trademark notices
MITRE Corporation Terms of Use

About Kaspersky Industrial CyberSecurity for Networks

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

Kaspersky Industrial CyberSecurity for Networks performs the following functions:

- Protects company assets by monitoring its industrial network devices. Detects device activity and device information based on data received from network packet analysis and/or from Kaspersky applications that perform functions to protect workstations and servers.
- Controls devices and interaction between them with respect to their MAC addresses or IP addresses affiliation with address spaces.
- Scans communications between industrial network devices to check their compliance with defined Interaction Control rules. Interaction Control rules can be generated automatically by running the application in learning mode.
- Displays interactions between industrial network devices as a network interaction map. Displayed objects are visually distinguished based on various attributes (for example, objects with issues).
- Displays a diagram of the physical connections between devices in an industrial network as a topology map. Displayed objects are visually distinguished by various attributes (for example, by the status).
- Detects risks based on traffic analysis and received information on devices.
- Enables device security auditing using vulnerability and compliance audit, configuration control, and active polling jobs.
- Extracts the parameter values of the technological process controlled by the Industrial Control System (hereinafter referred to as the "ICS") from network packets and checks the acceptability of those values based on the defined Process Control rules. Process Control rules can be generated automatically by running the application in learning mode.
- Monitors traffic to detect system commands that are transmitted or received by devices involved in process automation. Provides notifications regarding detected unauthorized system commands or situations that could be signs of industrial network security violations.
- Monitors project read and write operations for programmable logic controllers using data from industrial network traffic.
- Analyzes industrial network traffic for signs of attacks without affecting the industrial network or drawing the attention of a potential attacker. Uses Intrusion Detection rules, intrusion detection methods based on built-in algorithms, and Network Anomaly Detection rules to detect signs of attacks.
- Registers network sessions created by the devices for connecting with other devices.
- Registers events and relays information about them to recipient systems and to Kaspersky Security Center.

- Analyzes registered events and, upon detecting certain sequences of events, registers incidents based on embedded correlation rules. Incidents group events that have certain common traits or that are associated with the same process.
- Saves traffic associated with registered events in the database. Traffic can be saved automatically (if autosave is enabled for the traffic of events) or by requesting to download traffic.
- Receives, processes, and provides data from the applications that are part of the Endpoint Protection Platform (EPP). Provides the capability to trigger response actions on devices using EPP applications.
- Monitors hardware, user, application, patch, executable, and other configuration type lists on devices using data from various sources. Kaspersky Industrial CyberSecurity for Networks logs events whenever these lists are modified.
- Provides reports on the device status and system security, as well as the results of a security audit.
- Provides the capability to download traffic from the storages of the traffic dump files. Both the internal node storage (created automatically) and the external node storage, if connected on the node, can be used to download traffic.
- Can be used to work with both the GUI and API.
- Provides data for centralized monitoring of systems with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console.

Distribution kit

The distribution kit of Kaspersky Industrial CyberSecurity for Networks 4.5 includes the following files:

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

- Copies of files contained in the kics4net-release_<application version>.tar.gz archive:
  - Packages for installing Kaspersky Industrial CyberSecurity for Networks administration plug-in for Kaspersky Security Center and Kaspersky Industrial CyberSecurity for Networks administration web plug-in for Kaspersky Security Center Web Console
  - Files containing the text of the End User License Agreement in the supported localization languages: English and Russian
  - Files containing the text of the Privacy Policy in the supported localization languages: English and Russian
  - Files containing version information (Release Notes) in the supported localization languages: English and Russian

The distribution kit of Kaspersky Industrial CyberSecurity for Networks 4.5.1 includes the following files:

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

Hardware and software requirements

Hardware requirements

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

- Computer that will perform Server functions:
  - CPU: Intel Core i7 or equivalent (highest single-core frequency configurations are recommended)
  - RAM: 32 GB
  - Free space on the hard drive: 500 GB (SSD is recommended)
- Computer that will perform sensor functions:
  - CPU: Intel Core i5 / i7 or equivalent (maximum core configurations are recommended)
  - RAM: 8 GB, and an additional 4 GB when using monitoring points on this computer (for any number of monitoring points)
  - Free space on the hard drive: 250 GB (SSD is recommended)

We recommend a distributed deployment with a Server and external sensors. Configure industrial network traffic to be sent to sensor monitoring points. Sensors reduce the load on the Application Server thanks to traffic preprocessing and data storage.

All industrial network traffic must be load-balanced across Servers and sensors for stable performance. The recommended maximum incoming traffic rates are 500 Mbit/s for a Server node and 250 Mbit/s for a Sensor node.

Avoid sending duplicate traffic to the Server or sensor node and correctly configure the network equipment to transmit a copy of the traffic (for examples of configuring port mirroring for some switch models, see the Appendix). When duplicate traffic is detected, the application automatically drops the duplicate network packets, which increases the load on the computer hardware resources and in some cases may slow down the traffic processing.

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

Example:
Two sensor monitoring points are being used, one of these receiving 100 Mbit/s, and the other, 200 Mbit/s. The bandwidth between the sensor and the Server in that case must be at least 151 Mbit/s (1+(200+100)/2=151).

Software requirements

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

- CentOS Stream 9 operating system.

  To install and configure the operating system, you can use the instructions in the Appendix.

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

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

- To install application components in the CentOS operating system, the following conditions must be fulfilled (fulfillment of the conditions is ensured by the actions completed during the final stage in the specified instructions for installing and configuring the operating system):

  - The glibc-langpack-zh package is installed (required only for Kaspersky Industrial CyberSecurity for Networks 4.5.1).
  - Chrony time synchronization package version 3.1 or later is installed.
  - The SELinux access control enforcement system is disabled.
  - The dnf-utils package is installed.
  - The compat-openssl package is installed.
  - The lttng-ust package with the LTTng library is installed.

- To ensure proper functioning of application components on the computer that will perform Server functions, the following conditions must also be fulfilled in the CentOS operating system (fulfillment of the conditions is ensured by the actions completed during the final stage in the specified instructions for installing and configuring the operating system):

  - The EPEL repository has been installed along with the Python® language interpreter packages python3-psycopg2, python3-cryptography, and python3-paramiko, which are necessary for the operation of connectors and data conversion scripts (if the connectors will work on other computers, the repository and packages must also be installed on those computers).

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

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

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

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

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

Supported versions of Kaspersky Security Center

Kaspersky Industrial CyberSecurity for Networks is compatible with the following versions of Kaspersky Security Center:

- Kaspersky Industrial CyberSecurity for Networks 4.5 is compatible with Kaspersky Security Center 15.1 (version 15.1.0.20748) and Kaspersky Security Center 16 Linux. Supported Kaspersky Security Center Network Agent version: 16.0.0-254.
- Kaspersky Industrial CyberSecurity for Networks 4.5.1 is compatible with Kaspersky Security Center 15.1 (version 15.1.0.22239) and Kaspersky Security Center 16.1 Linux. Supported Kaspersky Security Center Network Agent version: 16.1.0-6517.

Integration with EPP applications

Kaspersky Industrial CyberSecurity for Networks supports operation in the integration mode with the following applications that perform functions to protect workstations and servers (EPP applications):

- Kaspersky Industrial CyberSecurity for Nodes versions 4.0 and 4.5.

  Interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes 4.0 is facilitated by the Kaspersky Endpoint Agent installed on the devices. Supported Kaspersky Endpoint Agent version: 4.0. Interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Nodes 4.5 is facilitated by the software modules that are built into Kaspersky Industrial CyberSecurity for Nodes 4.5.

- Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 (version 1.5.0.2558 must be used for Kaspersky Industrial CyberSecurity for Networks 4.5) and version 2.0.

  Interaction between Kaspersky Industrial CyberSecurity for Networks and this application is facilitated by the software modules that are built into Kaspersky Industrial CyberSecurity for Linux Nodes.

The maximum integration mode capabilities are available when using Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0. Depending on the version of the EPP application that you are using, integration mode capabilities are not available for the following functionality of Kaspersky Industrial CyberSecurity for Networks:

- Receipt of threat development chain details for EDR incidents when using Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5.

- Management of any response actions when using Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5.

- Management of the response actions **Delete file**, **Terminate process**, and **Start process** if Kaspersky Industrial CyberSecurity for Nodes is being used.

- Patch management on devices when using Kaspersky Industrial CyberSecurity for Linux Nodes.

- Receipt of telemetry data via data diode using the MQTT protocol over TCP when Kaspersky Industrial CyberSecurity for Linux Nodes is being used.

- Receipt of telemetry data via data diode using the UDP protocol if you are using Kaspersky Industrial CyberSecurity for Linux Nodes version 1.5 or Kaspersky Industrial CyberSecurity for Nodes.

Integration with Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity for Networks supports integration with Kaspersky SD-WAN version 2.2 or later.

Security recommendations for Kaspersky Industrial CyberSecurity for Networks

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

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

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

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

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

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

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

To ensure the security of data transmission in the local intranet system, you are advised to regularly update the digital certificates being used. It is also recommended to replace the self-signed certificates that were created by default for connecting to the Server through the web interface and for connecting via the Kaspersky Industrial CyberSecurity for Networks API with digital certificates that were issued by trusted certification centers. Additionally, to maintain the application's certified status, we recommend using certified or officially approved cryptographic protection tools for enhanced protection of the following network connections:

- Between the machines with the application components (Server and sensors) installed
- To application components via the web interface
- By third-party systems to Kaspersky Industrial CyberSecurity for Networks via special software modules (connectors)
- From a dedicated Kaspersky Industrial CyberSecurity network to external networks

We recommend the following security controls when using application management tools:

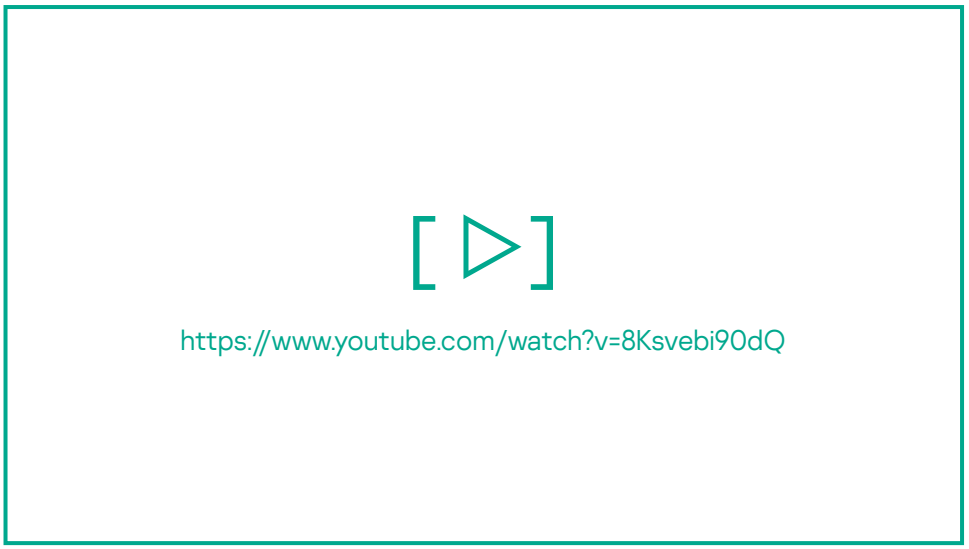
- Use account credentials that meet the requirements for user names and passwords of application user accounts.
- Ensure that passwords are confidential and unique.

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

  To force termination of a connection session, select **Log out** in the user menu.

What's new

Watch the video to learn about the new features of Kaspersky Industrial CyberSecurity for Networks 4.5.



https://www.youtube.com/watch?v=8Ksvebi90dQ

Overview of the main changes in 2025

Kaspersky Industrial CyberSecurity for Networks 4.5 has the following new capabilities and refinements:

- Added functionality for detecting network anomalies based on rules: Network Anomaly Detection rules are designed to analyze protocol attributes received in registered network sessions. Traffic anomalies, which can be detected using rules, allow you to identify complex targeted attacks within the perimeter, even in cases where traffic looks like normal network activity of devices to other traffic detection systems.

- On an integration server with EPP applications operating in TCP mode, the application does not allow you to disable verification of client authentication certificates if such certificates have been created. These certificates must be used to strengthen the security of client connections with the integration server. When adding an integration server or changing its settings, it is recommended to leave at least one created certificate for TCP mode so that the integration server can check the connected clients.

- Information can now be received about threat development chains for EDR incidents when working in integration mode with Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0.

- Expanded list of supported response actions: when working in integration mode with Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0, you can start all supported response actions, including the following new actions: **Delete file**, **Terminate process**, and **Start process**.

- Added support for industrial device hardware control for Siemens SIMATIC S7-1200 and S7-1500 devices and PLCs based on the CODESYS V3 platform (for example: Prosoft-Systems Regul R500).

- Added capability to set a password for connections to Schneider Electric Modicon M340/M580 devices as part of configuration control jobs and active polling jobs.

- Added support for the UDP protocol for receiving telemetry data from EPP applications via data diodes: to receive data via this protocol from Endpoint Agent components, UDP mode must be configured and enabled on the integration server.

- You can now receive mirrored traffic using the ERSPAN (Encapsulated Remote SPAN) technology. To do so, the node with the installed application component (Server or sensor) must serve as an endpoint for the created tunnels over the Generic Routing Encapsulation (GRE) protocol.

- Added functionality for monitoring device network behavior: you can fine-tune network interaction control or reset network behavior deviations for each device. If necessary, you can temporarily suspend monitoring of network interactions for individual devices.

- The lists of devices and data for which configurations can be received, saved, and compared within configuration control tasks have been expanded. New configuration types (previously called "configuration components") have been added for devices running Windows and Linux operating systems. Network devices of the Hirschmann RS20 and MACH series, Moxa EDS series, and Siemens RUGGEDCOM RSG2100 series have been added. Siemens SIMATIC S7-1200 and S7-1500 controllers and PLCs based on the CODESYS V3 platform (for example: Prosoft-Systems Regul R500) have been added.

- The list of roles for user accounts of the application has been expanded to include the following roles: **Security officer**, **Infrastructure expert**, and **ICS expert**.

- Added warning about insufficient free space for data storage: if the application detects that the amount of free space on the hard drive of a node is too low, a notification about this is displayed at the top of the web interface menu.

- Enhanced protection of Kaspersky Industrial CyberSecurity for Networks software modules to counteract various types of attacks (such as Local Privilege Escalation and other attacks).

Kaspersky Industrial CyberSecurity for Networks version 4.5.1 has the following new capabilities and improvements:

- The lists of devices for which configurations can be received, saved, and compared within Configuration Control jobs has been expanded to include network devices running the MikroTik RouterOS operating system and D-Link® devices of the DES and DGS series.

- Additional widgets have been added in the **Dashboard** section – when monitoring the system, you can now receive online information about the distribution of devices based on their statuses and about the distribution of traffic based on the detected protocols for the selected period.

- Simplified Chinese language is now supported.

Overview of Kaspersky Industrial CyberSecurity for Networks functionality

Kaspersky Industrial CyberSecurity for Networks functionality protects the infrastructures of industrial enterprises as part of a comprehensive set of solutions for ensuring industrial cyber resilience and security. You can read a description of the entire set of solutions and view information about the available tools for detecting and neutralizing threats at all levels of systems and networks of an industrial enterprise by visiting https://lp.kaspersky.com/global/industrialcyberresilience/

The application features are enabled by the appropriate parts of the Kaspersky Industrial CyberSecurity for Networks functionality. You can use the functionality selectively, according to the specific conditions and equipment level of your system. However, you achieve the most effective protection with Kaspersky Industrial CyberSecurity for Networks when you utilize the entirety of the provided functionality and configure it correctly.

Parts of the Kaspersky Industrial CyberSecurity for Networks functionality can be tentatively broken down into groups that ensure the features of the application are used as intended.

Asset Discovery

The following parts of the Kaspersky Industrial CyberSecurity for Networks functionality provide inventory of industrial network assets:

- Asset Management including the creation of a table of devices from device information contained in traffic that is received through monitoring points.
- Risk Control based on data contained in traffic, including detection of device vulnerabilities using device information.
- Active Device Polling to get the most accurate and complete information about devices and their configurations using active polling methods for both application-level protocols and common protocols.
- Online monitoring with widgets displaying system status.
- Network interaction map based on data from traffic coming through monitoring points, with the ability to view information about communications between devices in different periods of time.
- Topology Map that shows devices from the table of devices and connections added through active polling or manually.
- Network Sessions Monitoring including the creation of a network sessions table.
- Saving traffic dump files, which allows for subsequently downloading traffic to files, for example, network session traffic.

You can watch the tutorial video (see below) to familiarize yourself with the functionality.

https://www.youtube.com/watch?v=K012WnfC_os

Asset Discovery

Advanced asset management

Advanced asset management uses data requested and received by the following parts of the Kaspersky Industrial CyberSecurity for Networks functionality:

- Asset Management including enriching device information and adding new devices from data received from EPP applications.
- Device User Control based on the information received about accounts registered in the device operating systems.
- Device Application and Patch Monitoring based on information received about software installed and registered in the device operating systems.
- Device Executables Monitoring based on information received about executable file runs on devices.
- Interoperability with EPP applications for registering workstation and server security events, displaying communications between devices that have EPP applications installed, and receiving other network activity data.

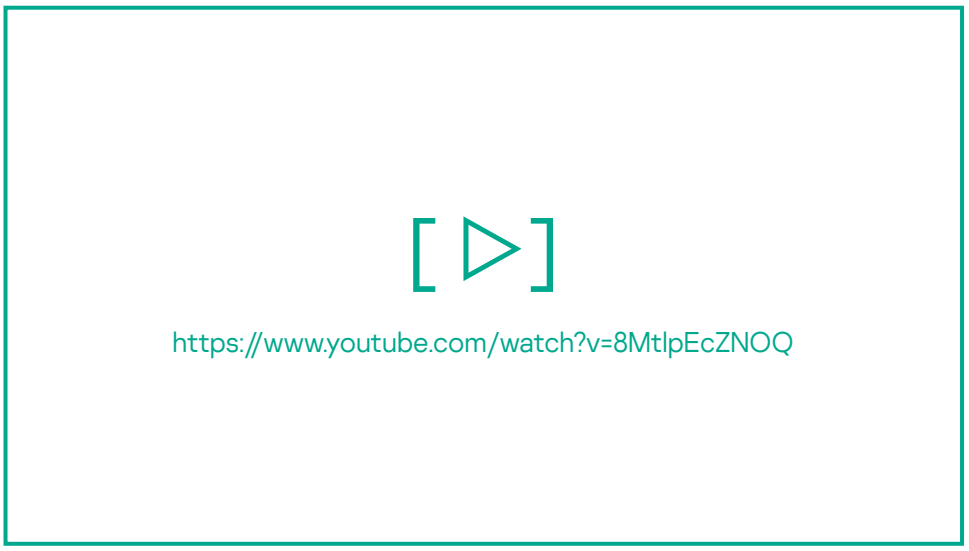
Security audit

Device security audit uses data requested and received by the following parts of the Kaspersky Industrial CyberSecurity for Networks functionality:

- Vulnerability and Compliance Audit to evaluate the compliance of device settings with security standards, and to search for vulnerabilities.
- Configuration Control to get and save detailed information about device configurations, and to compare changes in configurations.

- Active device polling for security audit purposes and to check devices for risks.
- Risk Control following vulnerability and compliance audit jobs and active device polling jobs.

You can watch the tutorial video (see below) to familiarize yourself with the functionality.



Security audit

Threat and Anomaly Detection

Threat and Anomaly Detection is provided by the following parts of the Kaspersky Industrial CyberSecurity for Networks functionality:

- Detection of intrusions, attacks, and various anomalies by using Intrusion Detection rules, Intrusion Detection methods based on built-in algorithms, and Network Anomaly Detection rules.
- Interaction Control for detecting unauthorized network interactions that do not comply with Network Integrity Control rules.
- Deep Packet Inspection (also referred to as Process Control below) for monitoring process parameters in traffic according to process control rules, and for monitoring system commands being sent. You can specify system commands allowed for sending in Interaction Control rules that use Command Control.
- Event Monitoring, registered based on various technologies and according to descriptions of attack techniques in the MITRE ATT&CK knowledge base, and which subsequently logs incidents according to Endpoint Detection and Response correlation rules.

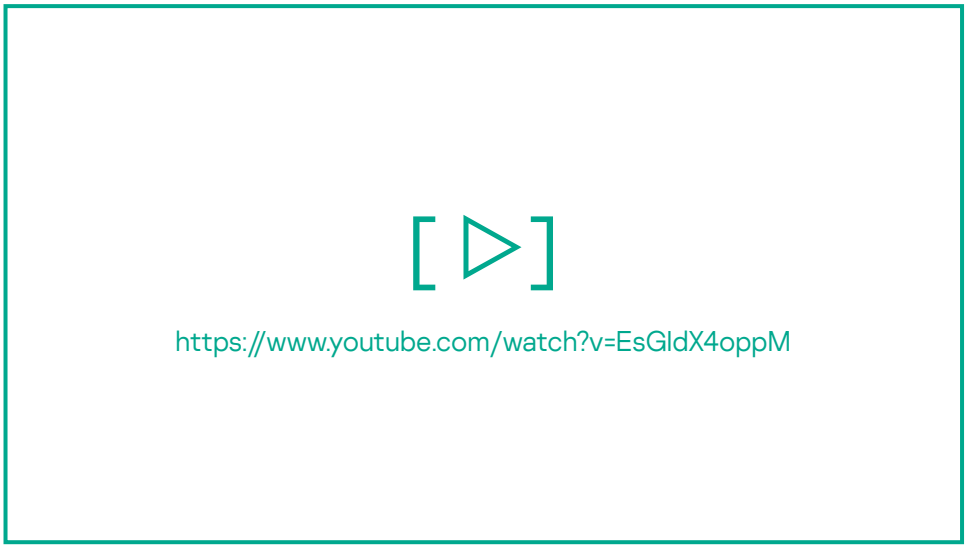
For in-depth analysis of industrial network traffic and early detection of anomalies, you can use Kaspersky Machine Learning for Anomaly Detection connectors.

Extended Threat Detection and Response

Extended Detection and Response (XDR) is provided by the following parts of Kaspersky Industrial CyberSecurity for Networks functionality:

- EDR incident information display when monitoring events to determine the status of detection processing and analyze threat evolution. The information is displayed as an activity graph and in a tabular format.
- Event enrichment with information about applications that were running when event registration conditions occurred, users who started applications, and other information.
- Manage response actions on devices that have Endpoint Agent installed. Depending on the action trigger conditions, you can enable device network isolation, prevent files from running, terminate and start processes, and delete or quarantine files.
- Automatically block network access for unauthorized devices by using network switch connectors.

You can watch the tutorial video (see below) to familiarize yourself with the functionality.



https://www.youtube.com/watch?v=EsGldX4oppM

Threat detection, analysis and response

Ecosystem and Integrations

You can configure Kaspersky Industrial CyberSecurity for Networks to interoperate with the following Kaspersky applications and solutions:

- Kaspersky Security Center.
- EPP applications provided by Kaspersky Industrial CyberSecurity for Nodes or Kaspersky Industrial CyberSecurity for Linux Nodes.
- Kaspersky SD-WAN.

Additionally, you can use connector and Kaspersky Industrial CyberSecurity for Networks API functionality for interoperation with many other applications and solutions including third-party products. For example, interoperation with the following software products is supported:

- Kaspersky Unified Monitoring and Analysis Platform.
- Kaspersky Machine Learning for Anomaly Detection.
- Cisco™ switches.

If you want Kaspersky Industrial CyberSecurity for Networks to interoperate with software products not supported by the built-in connectors, you can add new connector types to the application.

Application architecture

Kaspersky Industrial CyberSecurity for Networks includes the following components:

- The *Server* is the main component that receives data, processes it, and provides it to users of the application. The received information (such as events and device information) is saved on the Server in the database. Only one Server can be used in each Kaspersky Industrial CyberSecurity for Networks deployment scenario.

- A *sensor* is a component that is managed by the Server and receives and analyzes data from computer networks that are connected to the network interfaces of the sensor's computer. A sensor forwards the data analysis results to the Server. Based on the specific requests from the Server, the sensor can forward data in the same format in which the data was received for analysis (for example, traffic related to registered events). Sensors are installed on separate computers. A sensor cannot be installed on a computer that performs Server functions. The application can have up to 50 sensors.

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

If Kaspersky applications that perform workstation and server protection functions (EPP applications) are installed on the computers of the monitored network, you can configure integration with these applications in Kaspersky Industrial CyberSecurity for Networks. After configuring the integration, the Server and/or sensors receive data from EPP applications and can interact with them.

When using security audit jobs, the Server and/or sensors can remotely connect to the devices to scan and receive results.

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

- Manages sensors and receives from them the results of analyzing the received data.

- Processes and saves received information about devices and their interactions.

- Registers and saves events.

- Conducts an additional analysis of accumulated information to detect threats and incidents (for example, according to event correlation rules).

- Monitors application performance.

- Monitors the activities of application users.

- Processes incoming requests submitted through the web interface and connectors, and provides the requested data.

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

- Analyzes incoming industrial network traffic:

  - Extracts information about device communications and process parameters from traffic.

  - Identifies signs of attacks in traffic.

- Registers events based on the results of data analysis.
- Relays events, information about traffic, device information, and process parameters to the Kaspersky Industrial CyberSecurity for Networks Server.

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

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).

Kaspersky Industrial CyberSecurity for Networks supports receipt of mirrored traffic, including using Encapsulated Remote SPAN (ERSPAN) technology. If ERSPAN technology is employed, the node with the installed application component (Server or sensor) acts as an endpoint for the created tunnels using the Generic Routing Encapsulation (GRE) protocol. For more information, you can contact Technical Support.

The application has the following restrictions on the number of monitoring points:

- Total number of monitoring points: a maximum of 50
- Monitoring points on the Server: a maximum of 4
- Monitoring points per sensor: a maximum of 8

When running integrated with Kaspersky SD-WAN, a maximum of 100 monitoring points can be used per node or in total on all nodes that have application components installed on them.

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

- Kaspersky Industrial CyberSecurity for Networks Server node.
- Kaspersky Industrial CyberSecurity for Networks sensor nodes.
- Computers for connecting to the Server and sensors through the web interface.
- Computers with Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes and the Endpoint Agent software components.
- Devices to which remote connections are established for scanning as part of security audit jobs.
- Computers hosting connector application modules.
- Computer hosting Kaspersky Security Center.
- Network switch.

Common deployment scenarios

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

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

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

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

Installing a Server without external sensors

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

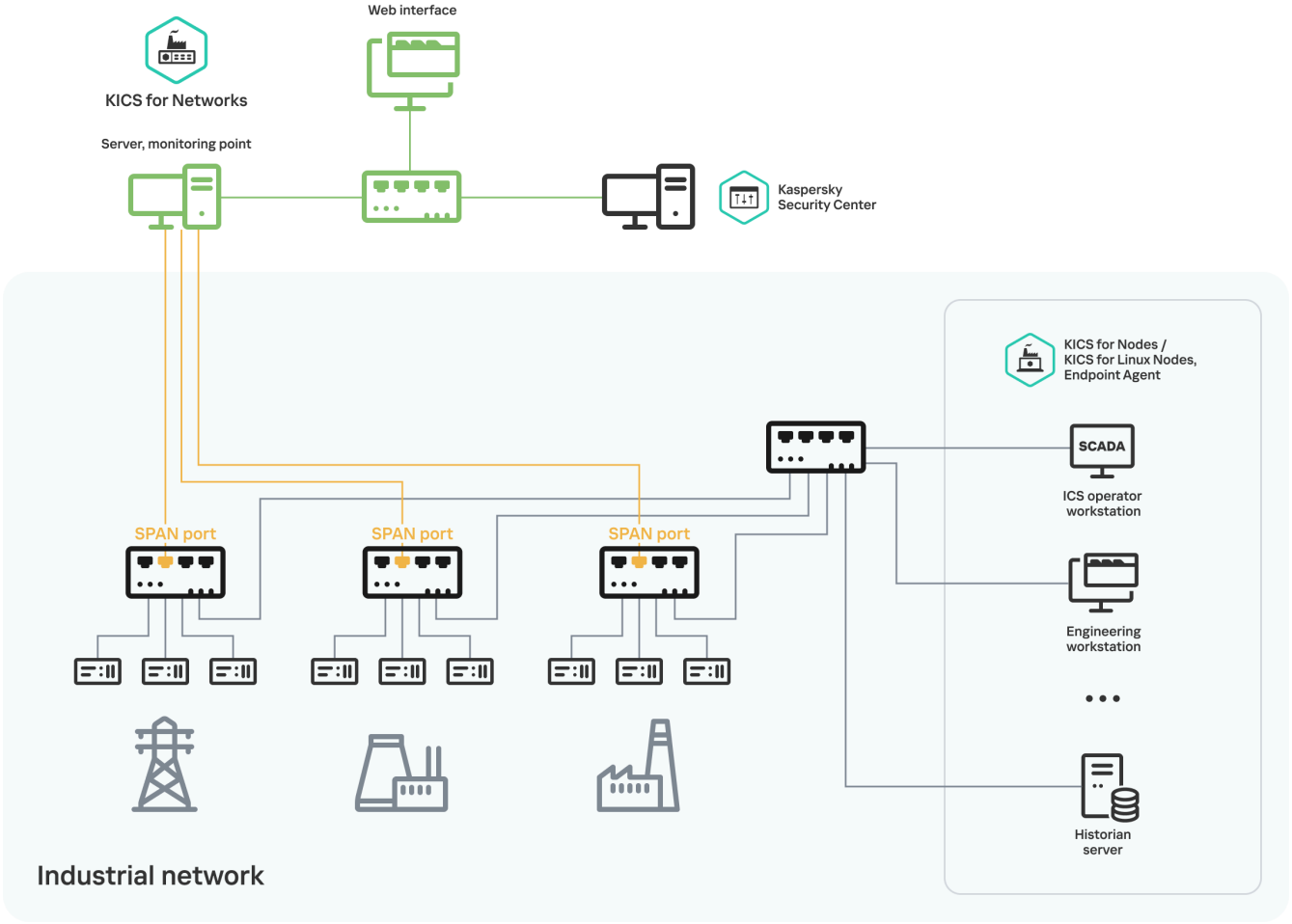
It is recommended to choose the Server deployment scheme without external sensors for monitoring one site with a small number of traffic sources. In the case of a distributed network architecture, it is recommended to choose the Server and external sensors deployment scheme.

If traffic aggregation tools (such as aggregation switches or network packet brokers) are used to transmit traffic to the Server in a distributed network architecture, important data about the origination sources of information security events may be lost. In addition, if the same device addresses are used in different network segments, these addresses cannot be correctly matched to the devices without additional configuration of traffic aggregation tools and the application. Also, individual network segments and devices may not be available for monitoring in the application, and errors may occur when using some application functions (in particular, the functionality of auditing, active polling, and response to threats).

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

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

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



Example deployment of a Server without sensors

Installing a Server and external sensors

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

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

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

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

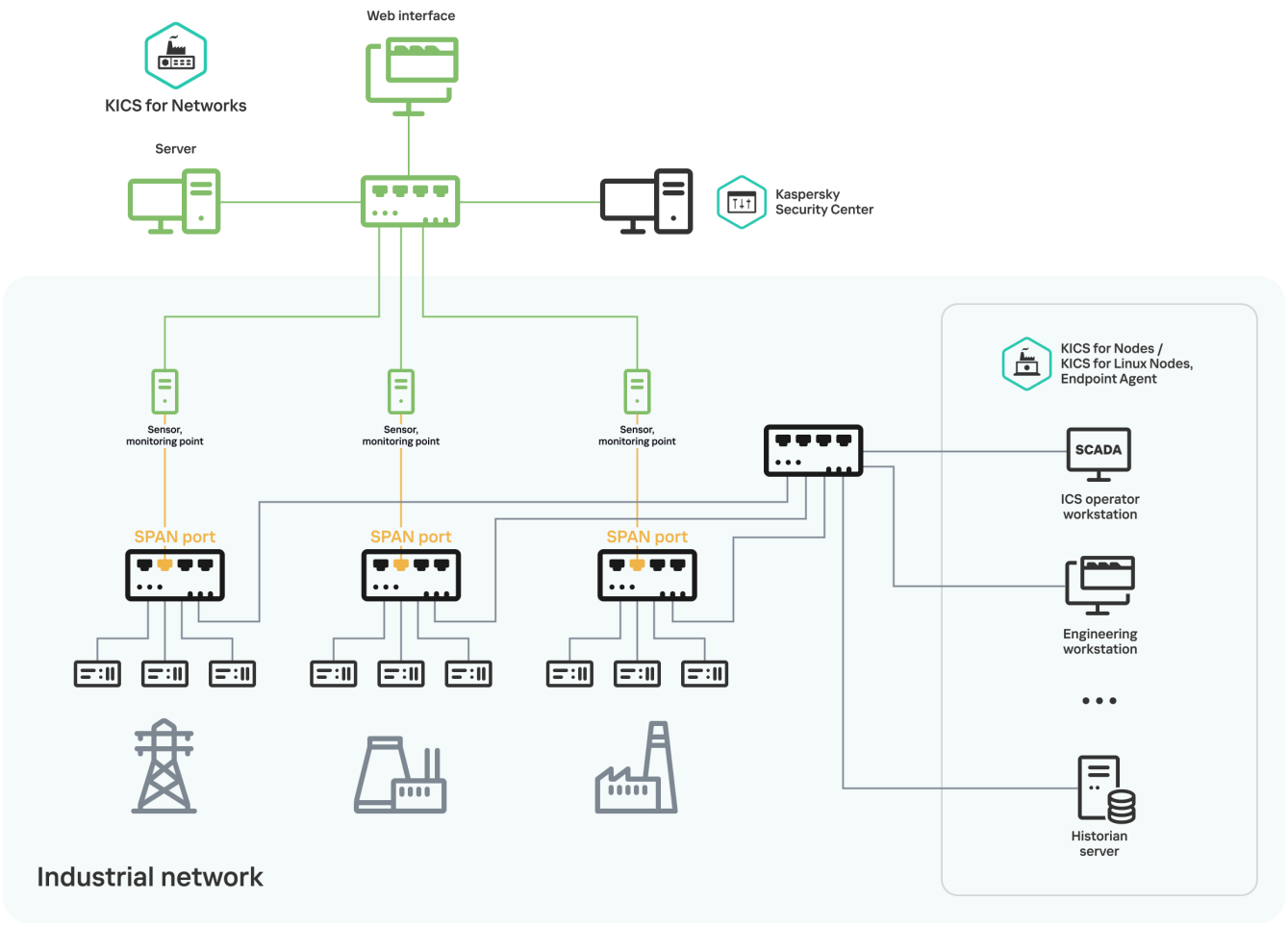
Computers must also have separate network interfaces that will be used for the following purposes:

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

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

It is recommended to install the Kaspersky Industrial CyberSecurity for Networks sensors near the traffic sources and/or in the same network segments where Kaspersky Industrial CyberSecurity for Nodes and/or Kaspersky Industrial CyberSecurity for Linux Nodes are installed. This approach simplifies the configuration of integration between applications, does not require additional steps to set up device access and access to configuring the network equipment, and minimizes network connections between various segments.

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



Example deployment of a Server and three sensors

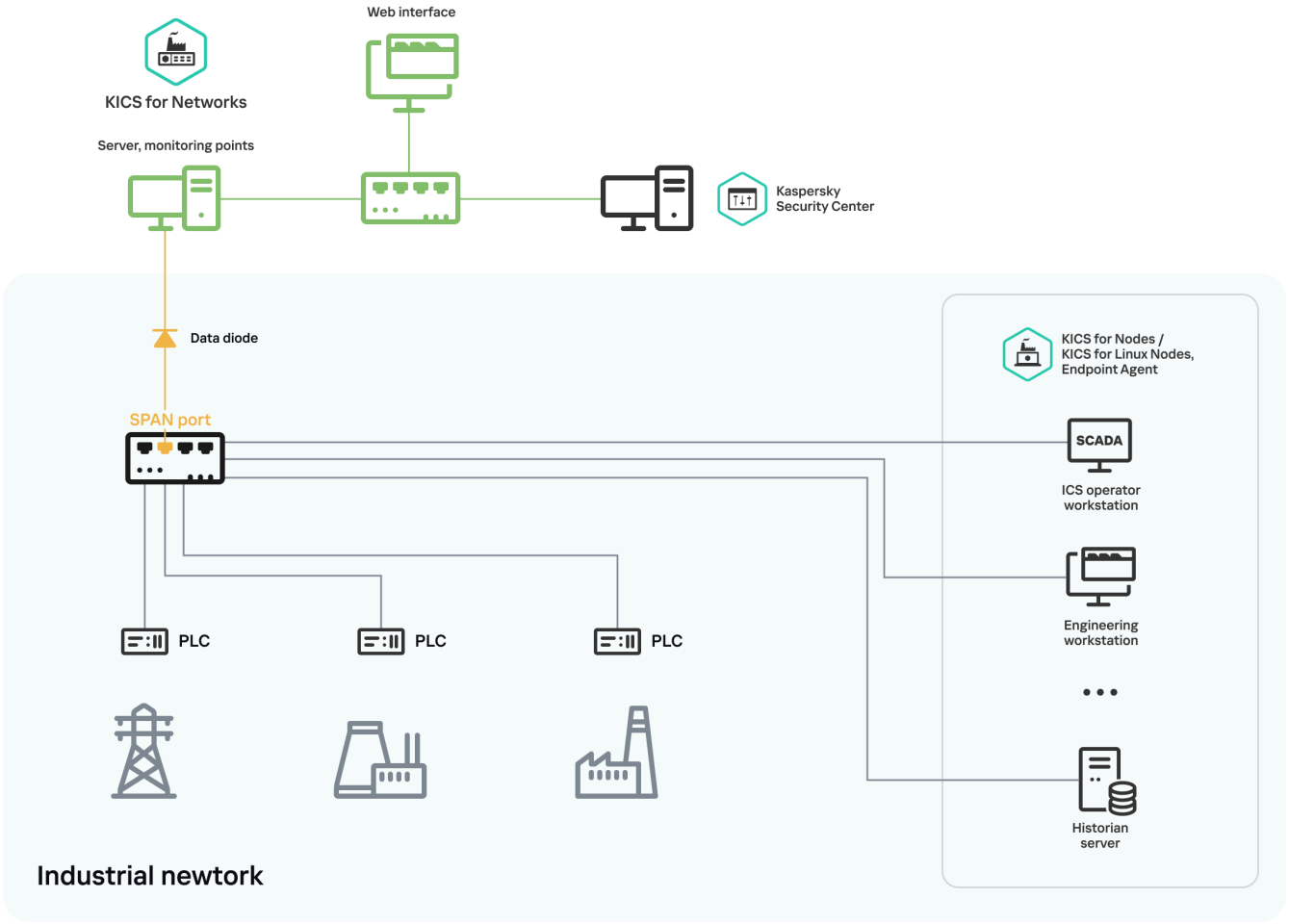
Connecting Kaspersky Industrial CyberSecurity for Networks to an industrial network via data diodes

To connect Kaspersky Industrial CyberSecurity for Networks to an industrial network, you can additionally use special devices that provide unidirectional transmission of data from the industrial network. These devices are called *data diodes*.

Receiving industrial network traffic via data diodes

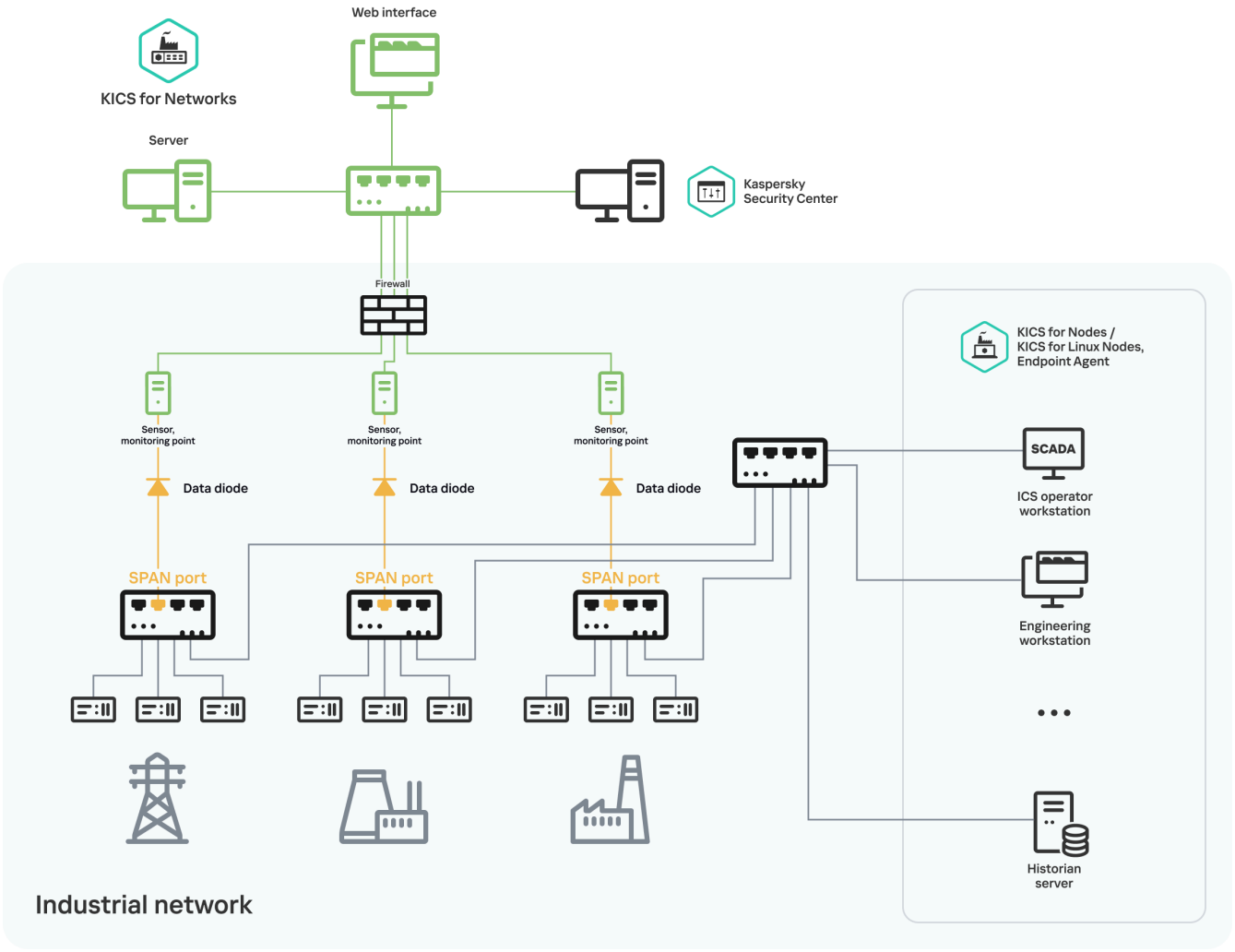
To transmit industrial network traffic to Kaspersky Industrial CyberSecurity for Networks, data diodes must support unfiltered transmission of network packets for all link layer protocols, including service protocols. Data diodes are installed on the connection links of Kaspersky Industrial CyberSecurity for Networks monitoring points and on SPAN ports of network switches.

The figure below shows a deployment scenario with a connection to a monitoring point on the Server via a data diode. The data diode transfers traffic from a SPAN port of a network switch in an industrial network. In this scenario, the Server is installed without external sensors.



Standard scenario for connecting the Server via a data diode

The figure below shows a deployment scenario where several Kaspersky Industrial CyberSecurity for Networks sensors are connected via data diodes. The data diodes transfers traffic from SPAN ports of network switches in an industrial network. In this scenario, the Server is installed with three sensors.



Standard scenario for connecting sensors via data diodes

If you want to additionally separate the segments of the industrial network where the sensors are installed, from the segment of the Kaspersky Industrial CyberSecurity dedicated network where the Server is installed, you can use a firewall on the connection links between the sensors and the Server.

Receiving telemetry data from EPP applications via data diodes

Endpoint Agent software components that interact with EPP applications can send telemetry data via data diodes. Telemetry data must be received by Kaspersky Industrial CyberSecurity for Networks nodes via network interfaces that are not being used as monitoring points. Therefore, to simultaneously receive telemetry data and industrial network traffic, you will need to install separate data diodes connected to the corresponding network interfaces of Kaspersky Industrial CyberSecurity for Networks nodes. Telemetry data must be sent to ordinary network interfaces, and traffic from SPAN ports must be sent to the network interfaces of monitoring points.

Depending on the versions of the EPP applications, Endpoint Agent components can send telemetry data via data diodes using the following protocols:

- MQTT over TCP

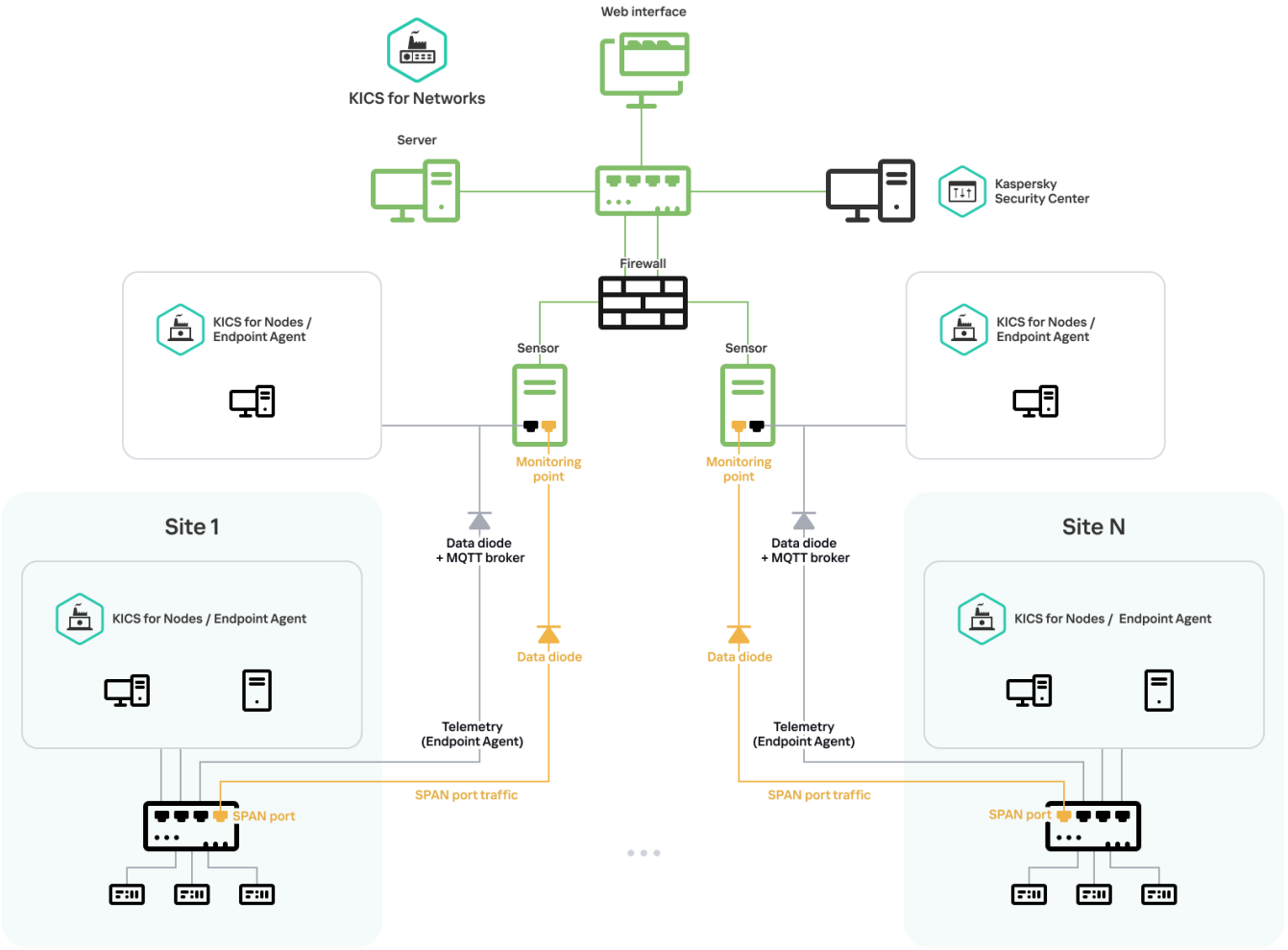
  This protocol is used when working in integration mode with Kaspersky Industrial CyberSecurity for Nodes. For detailed information on configuring an EPP application for this data transfer method, please refer to the appropriate Help system: Kaspersky Industrial CyberSecurity for Nodes 4.5 or Kaspersky Endpoint Agent 4.0.

- UDP

  This protocol is used when working in integration mode with Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0. For detailed information on configuring an EPP application for this data transfer method, please refer to the Help system of Kaspersky Industrial CyberSecurity for Linux Nodes 2.0.

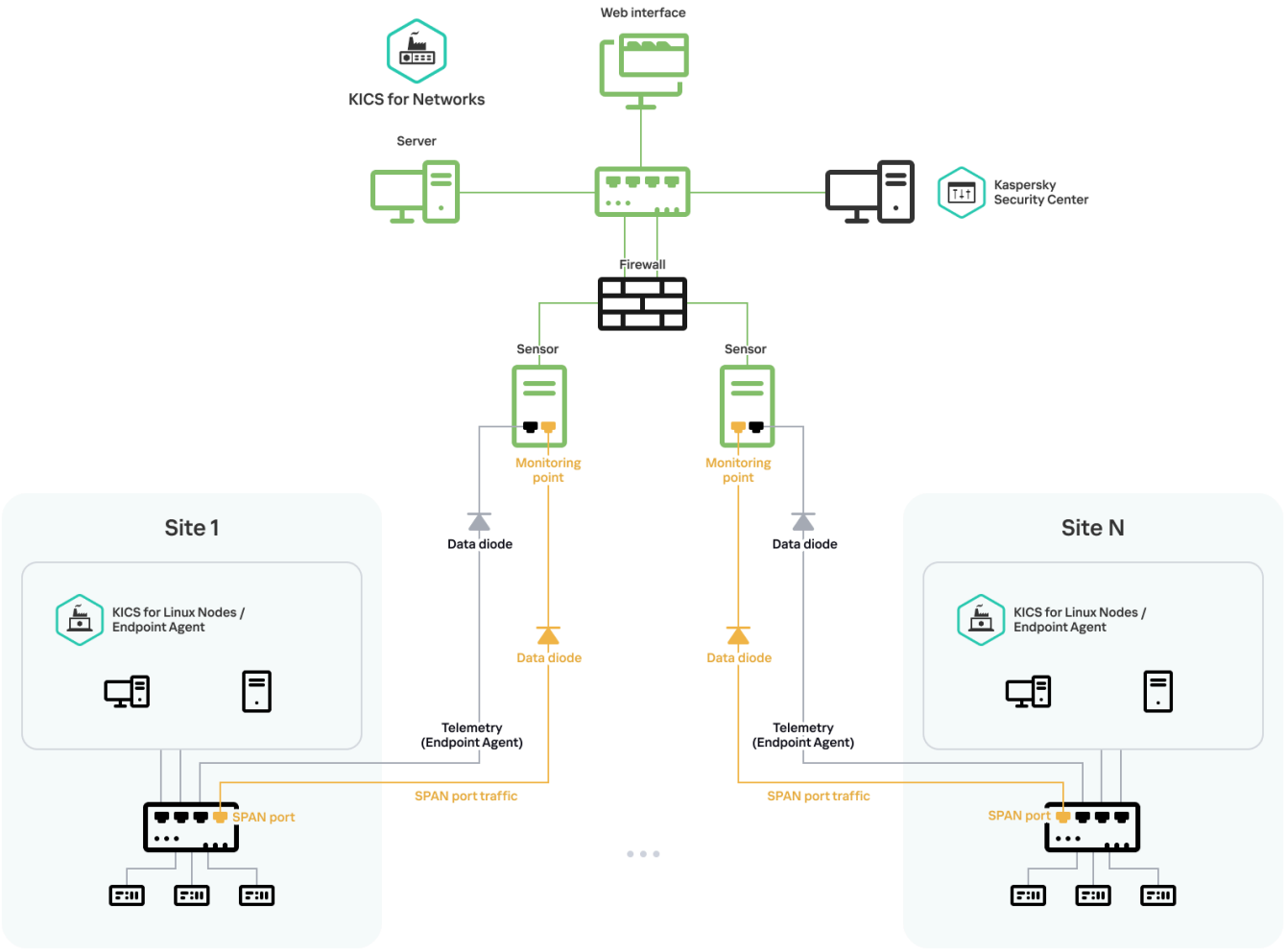
In Kaspersky Industrial CyberSecurity for Networks, integration servers facilitate the receipt of telemetry data from EPP applications. To receive data from Endpoint Agent components, the mode corresponding to the utilized data transfer protocol (TCP mode or UDP mode) must be configured and enabled on the integration server.

The figure below shows the deployment scenario for receiving telemetry data from EPP applications via the MQTT protocol over TCP and traffic sent from SPAN ports of network switches from multiple industrial sites to Kaspersky Industrial CyberSecurity for Networks sensors. In this scenario, telemetry data is transmitted in MQTT messages. To transmit MQTT messages via data diode, this diode must support MQTT broker functionality. To receive and process MQTT messages after the data diode, you must use additional subscriber computers that have EPP applications installed.



Receiving traffic and data from EPP applications using the MQTT protocol over TCP

The figure below shows the deployment scenario for receiving telemetry data from EPP applications via the UDP protocol and traffic sent from SPAN ports of network switches from multiple industrial sites to Kaspersky Industrial CyberSecurity for Networks sensors. This scenario does not require additional subscriber computers with EPP applications installed.



Receiving traffic and data from EPP applications over UDP

Receiving industrial network traffic from Kaspersky SD-WAN components

Kaspersky Industrial CyberSecurity for Networks can run integrated with Kaspersky SD-WAN. When running in this mode, Kaspersky Industrial CyberSecurity for Networks receives mirrored traffic that passes through switches on remote sites if a Customer Premise Equipment (CPE) device, a Kaspersky SD-WAN component, is installed on these sites. You can use CPE devices to implement some features of Kaspersky Industrial CyberSecurity for Networks sensors by forwarding industrial network traffic from remote sites to the application. The data is sent to the application via secure channels.

CPE devices that receive mirrored traffic directly on remote sites encrypt the traffic to forward it to other (receiving) CPE devices that share a network with Kaspersky Industrial CyberSecurity for Networks nodes. Receiving CPE devices must be assigned the SD-WAN gateway role if communication between devices that send mirrored traffic is only allowed through the gateway. We recommend placing receiving CPE devices on a dedicated Kaspersky Industrial CyberSecurity network. These devices relay mirrored traffic to the network interfaces of Kaspersky Industrial CyberSecurity for Networks nodes.

Traffic received at the network interface of the Kaspersky Industrial CyberSecurity for Networks node from various CPE devices is identified by virtual local area network (VLAN) IDs added to network packets in accordance with the IEEE 802.1q standard. When configuring an integration between Kaspersky Industrial CyberSecurity for Networks and Kaspersky SD-WAN, ensure that the VLAN IDs used by the Kaspersky SD-WAN components match those used by the computer with the Kaspersky Industrial CyberSecurity for Networks component installed. Each network interface receiving traffic with a certain VLAN ID must be the VLAN interface with the matching ID.

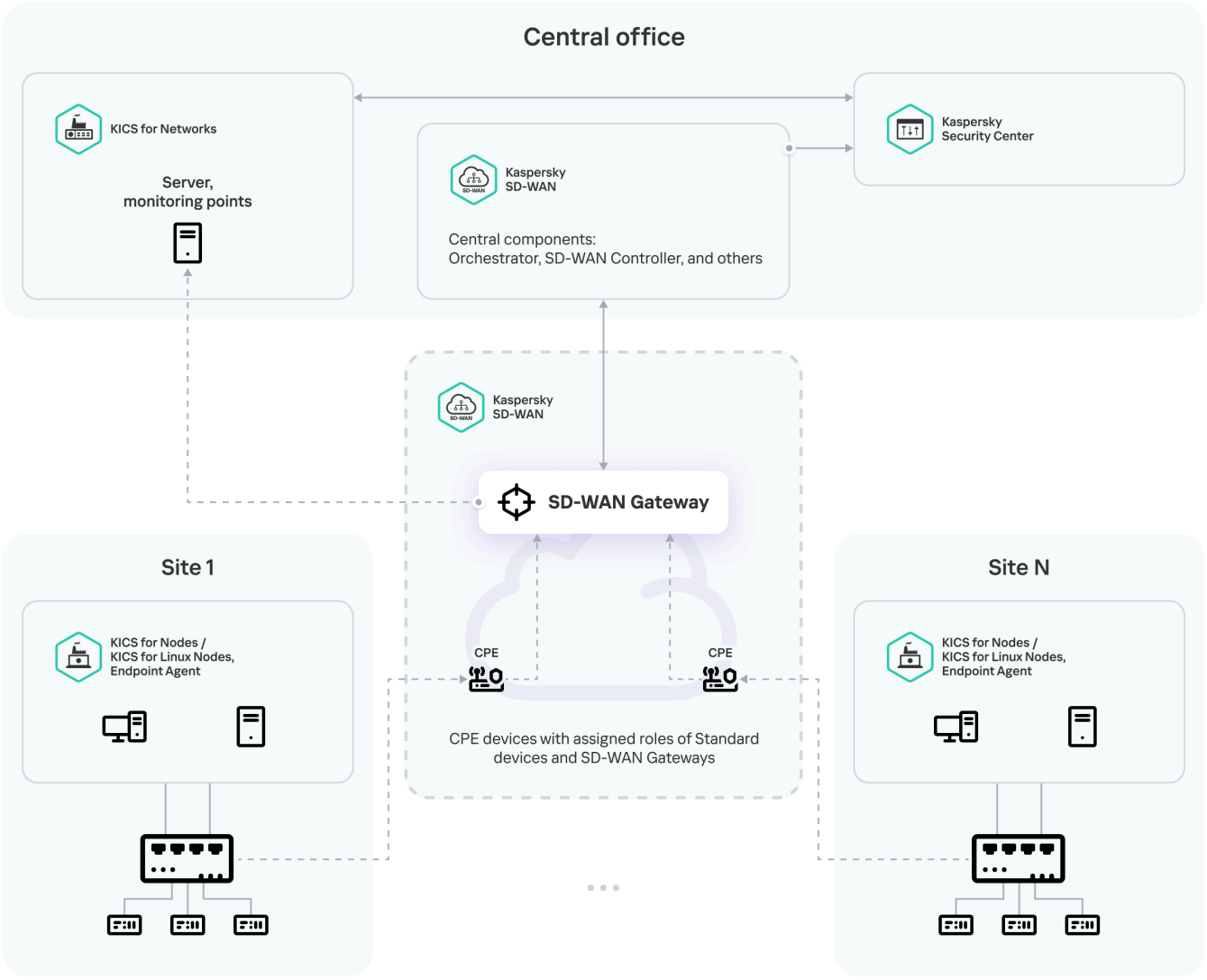
For efficient integration, you can relax the restrictions on the number of monitoring points in the application through additional configuration of the software components. Maximum possible restrictions on integration with Kaspersky SD-WAN:

- A maximum of 100 monitoring points per node
- Total, no more than 100 monitoring points in the application

The rest of the requirements for deployment of Kaspersky Industrial CyberSecurity for Networks components are similar to other typical deployment patterns, such as Server installation without external sensors.

For more information about configuring software components to run in integration mode, contact your technical account manager (TAM).

The figure below shows an example deployment pattern for Kaspersky Industrial CyberSecurity for Networks and Kaspersky SD-WAN for when mirrored traffic from multiple sites travels to the Kaspersky Industrial CyberSecurity for Networks Server through a single SD-WAN gateway. Computers connected to the dedicated Kaspersky Industrial CyberSecurity network and computers with central SD-WAN components installed are located in the corporate headquarters. The dotted lines designate the path that the mirrored traffic takes from the switches on the remote sites.



Example of a deployment pattern that includes Kaspersky SD-WAN

Getting started: basic scenario

To deploy Kaspersky Industrial CyberSecurity for Networks, you can use the sequence of steps in this Help article. By clicking the links in each step, you can proceed to the corresponding Help articles containing detailed descriptions.

1 Preparing for installation

1.1 →	1.2 →	1.3 →
Selecting a deployment scenario	Selecting a centralized or local installation	Preparing computers for centralized or local installation

1.4 →	1.5
Preparing network switches for traffic duplication to SPAN ports	Configuring the availability of utilized ports and protocols

2 Installation and initial configuration

2.1 →	2.2 →	2.3 →
Centralized or local installation and update	Hardening the security of computers after installing the application	Configuring a firewall on nodes

2.4 →	2.5 →	2.6
Configuring time synchronization on nodes	Installing the administration plug-in for Kaspersky Security Center	Initial configuration of the application after installation

3 Getting started

3.1 →	3.2 →	3.3 →
Adding and connecting sensors	Adding application users	Adding a license key

3.4 →	3.5 →	3.6 →
Configuring interaction with Kaspersky Security Center	Starting the installation of updates and configuring automatic updates	Adding monitoring points

3.7 →

Enabling technologies and training the application

3.8 →

Adding connectors for interaction with third-party systems

3.9

Configuring the main functionality of the application:

- Integration with EPP applications
- Asset Management
- Process control
- Interaction control
- Detection rules
- Security audit

After completing the steps to deploy Kaspersky Industrial CyberSecurity for Networks, you are advised to familiarize yourself with the application's capabilities for saving the accumulated data and defined settings. For example, you can configure log storage settings, connect external storage for traffic dump files, export and import a security policy, and save and load a backup copy of data using the kics4net-backup.sh data migration script. For descriptions of the application settings, see the Administration of Kaspersky Industrial CyberSecurity for Networks Help section.

While using the application, users have access to actions depending on their assigned roles. Check out the functionality for accomplishing the following core tasks of application users:

- Monitoring the system in widgets
- Viewing the network map
- Monitoring network sessions
- Monitoring events
- Monitoring tag values
- Getting reports
- Controlling risk, and detecting default passwords and insecure encryption protocols used on devices
- Initiating response actions
- Monitoring the state of the application

Installing and removing the application

This section contains instructions on preparing for the installation of Kaspersky Industrial CyberSecurity for Networks, installing, updating, and removing application components. This section also provides instructions on how to perform the recommended actions after installing the components.

You can install, update, and remove application components either centrally or locally. The appropriate method for performing these actions depends on the readiness of the network infrastructure, the remoteness and availability of computers, and the previously selected method for installing application components (for update or removal actions).

After selecting the deployment scenario for Kaspersky Industrial CyberSecurity for Networks, you can use the application component installation method that is appropriate for you depending on the following conditions:

- Centralized installation lets you remotely install the Server and sensor components on different computers by using one control node and performing the procedure one time. To connect the control node to computers, SSH protocol access must be opened on these computers. You must keep in mind that the installation packages of the application will be sent to computers over the network, which may take some time over slow communication channels.

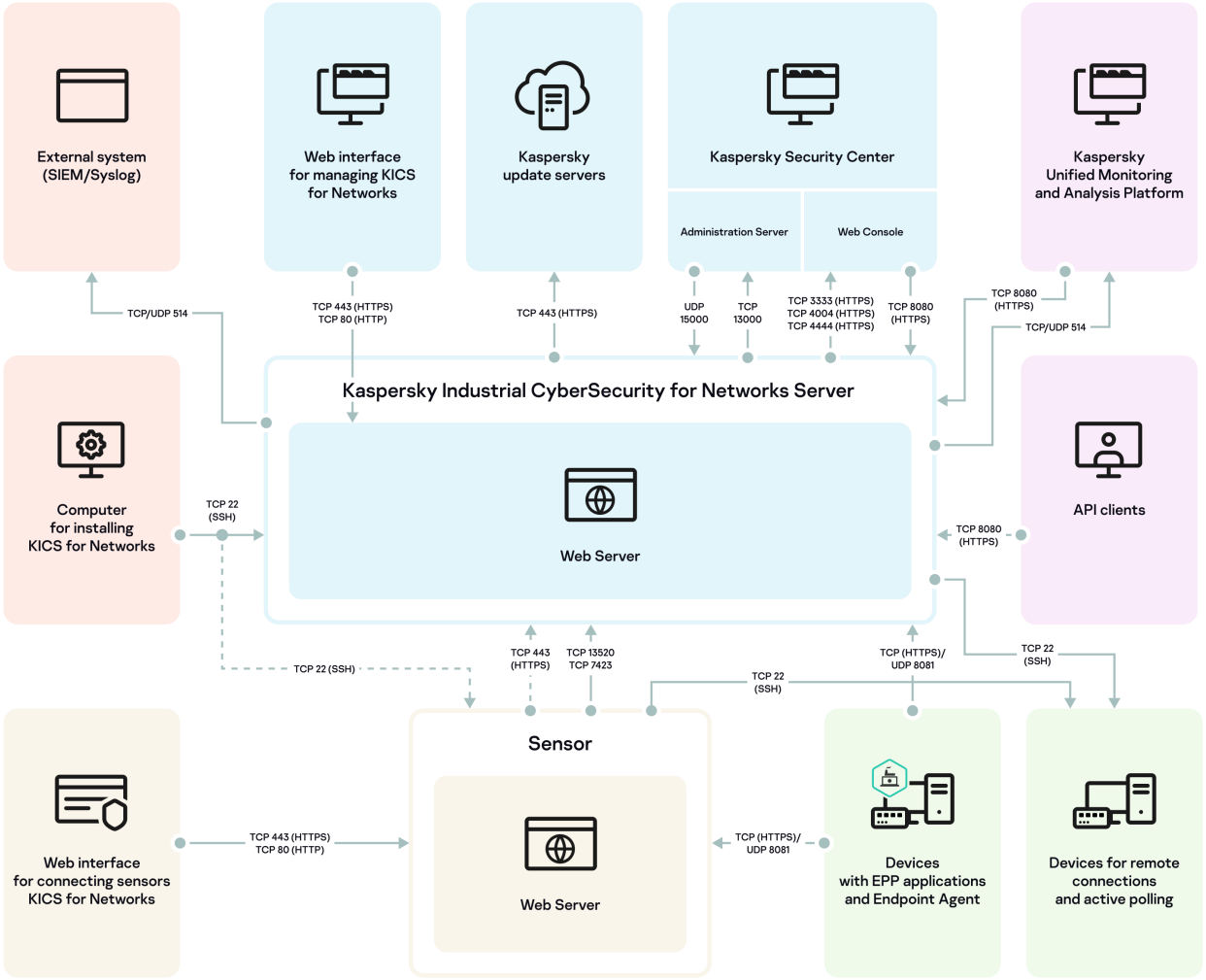
- Local installation is the convenient option to use if, for example, you need to prepare the Server nodes and sensors in advance before sending them directly to industrial sites. This option also lets you install application components on-site in conditions where the computers have limited network availability. In this case, application components are installed on each computer separately.

Ports used for installation and operation of components

To ensure successful installation and operation of components of Kaspersky Industrial CyberSecurity for Networks, specific ports and protocols that will be used for data transfer must be available. You need to configure use of these ports and protocols in the settings of your network hardware or software that will be used to monitor network traffic. In particular, after installing the Server and sensors, additional configuration of the firewall on these computers may be required for the corresponding functionality to work.

If the necessary ports and protocols are blocked by network equipment or software, Kaspersky Industrial CyberSecurity for Networks cannot use the functionality that requires these ports for network interactions. For example, if TCP/UDP port 514 is not available for the Server computer, the application will not be able to send data through the **Syslog** and **SIEM** connectors.

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



Utilized ports and protocols

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

Purpose of utilized ports

Port	Protocol	Description
Computer where application components are installed		
22	TCP (SSH)	This port is used to connect to nodes and to install Server and sensor components.
Computer that performs Server functions		
22	TCP (SSH)	This port is used for the following purposes: • Interaction with the computer where application components are installed • Remote or connector-assisted connection to devices for scans as part of security audit jobs
80	TCP (HTTP)	This port is used for connecting through the web interface.
443	TCP (HTTPS)	This port is used for the following purposes: • Connection through the web interface • Connection to Kaspersky update servers • Connection of a sensor through the web interface automatically over the network
514	TCP/UDP	This port is used to send data through **Syslog** and **SIEM** connectors.

Port	Protocol	Description
3333 4004 4444	TCP (HTTPS)	Used for interaction with the Identity and Access Manager component in Kaspersky Security Center Web Console when using the single sign-on (SSO) technology.
7423	TCP	This port is used for connections of sensors.
8080	TCP (HTTPS)	This port is used for the following purposes: • Connection via the Kaspersky Industrial CyberSecurity for Networks API (including the KUMA connector) • Connecting Kaspersky Security Center Web Console
8081	TCP (HTTPS) / UDP	It is used to receive data from EPP applications if the integration server is enabled in TCP or UDP mode, respectively, on the Server node.
13000	TCP	This port is used to connect Network Agent to the Kaspersky Security Center Administration Server.
13520	TCP	This port is used for connections of sensors.
15000	UDP	Used to send the control signals to the Network Agent from Kaspersky Security Center Administration Server.
Computer that performs sensor functions		
22	TCP (SSH)	This port is used for the following purposes: • Interaction with the computer where application components are installed • Remote or connector-assisted connection to devices for scans as part of security audit jobs
80	TCP (HTTP)	This port is used for connecting through the web interface.
8081	TCP (HTTPS) / UDP	It is used to receive data from EPP applications if the integration server is enabled in TCP or UDP mode, respectively, on the sensor node.

Centralized installation and removal of application components

This section provides information on centralized installation and removal of application components from one computer. Centralized installation and removal of the Kaspersky Industrial CyberSecurity for Networks Server and sensors is performed using the script named kics4net-deploy-<application version number>.bundle.sh.

If you need to install or remove a specific component after already performing centralized installation, you can apply the local installation or removal scripts that are included in the application distribution kit.

The scenario for centralized installation of application components consists of the following steps:

1. **Fulfilling the requirements for centralized installation**

   At this step, make sure that the centralized installation requirements have been fulfilled.

2. **Preparing for application installation**

   At this stage, prepare the computers for centralized installation of Kaspersky Industrial CyberSecurity for Networks components.

3. **Centralized installation of application components**

   At this step, perform the centralized installation of application components using the script named kics4net-deploy-<application version number>.bundle.sh. Centralized installation is possible in the following modes:

   - Interactive mode. In this mode, run the kics4net-deploy-<application version number>.bundle.sh script and follow the instructions of the script.
   - Non-interactive mode. In this mode, prepare the installation settings file and run the kics4net-deploy-<application version number>.bundle.sh script with the `silent-mode` parameter.

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

4. **Reinforcing the security of computers with application components installed**

   After installing Kaspersky Industrial CyberSecurity for Networks, you are advised to harden the security of the operating systems on computers that have application components installed. Hardening of operating systems during centralized installation is performed using the script named kics4net-deploy-<application version number>.bundle.sh.

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

   If you need to use Kaspersky Security Center functions for working with Kaspersky Industrial CyberSecurity for Networks, install the Kaspersky Industrial CyberSecurity for Networks administration plug-in. The following administration plug-ins are provided:

   - Web management plug-in for Kaspersky Security Center Web Console - this plug-in is intended for use in Kaspersky Security Center Linux, as well as for advanced centralized control and single sign-on technology in Kaspersky Security Center Windows. Install this plug-in using one of the methods available in the Kaspersky Security Center Web Console interface.

   - Management plug-in for Administration Console based on Microsoft Management Console (MMC) - this plug-in is intended for use in Kaspersky Security Center Windows. Install this plug-in locally on the computer where the Kaspersky Security Center Administration Server is installed.

6. **Startup configuration of the application after Server installation**

   After installing the Server, complete the initial configuration in the web interface of Kaspersky Industrial CyberSecurity for Networks. After the initial configuration is completed, the web interface page will open in the normal operating mode of the application.

After installing the application components, prepare the application for operation.

Requirements for centralized installation of application components

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

- The computers meet the hardware and software requirements.
- The equipment, hardware, and software of the computers are compliant with all operational security recommendations.
- To ensure proper functioning of application components, use specially dedicated computers that only have software from the operating system installed.

  If third-party applications are installed on computers, the performance of components of Kaspersky Industrial CyberSecurity for Networks may be reduced.

- The computers have network access, and access over SSH is configured and open.
- The computers have user accounts with root privileges (application components will be installed under these user accounts).

- The computers do not have any user accounts or groups with the following names that are reserved for interaction between application components (if these accounts exist, they could receive elevated access rights, even root privileges, after the application is installed):
  - kics4net
  - kics4net-anomaly-hunter
  - kics4net-apm
  - kics4net-asset-config-repo
  - kics4net-asset-inventory
  - kics4net-blob-storage
  - kics4net-cli
  - kics4net-clickhouse
  - kics4net-config-control-orch
  - kics4net-connectors
  - kics4net-connectors-launcher
  - kics4net-email-gateway
  - kics4net-epp-proxy
  - kics4net-fts
  - kics4net-nats
  - kics4net-nats-server
  - kics4net-oval-facade
  - kics4net-postgresql
  - kics4net-report-builder
  - kics4net-report-data-source
  - kics4net-report-renderer
  - kics4net-report-tc
  - kics4net-report-tcv
  - kics4net-responses-manager
  - kics4net-risk-oval-detector
  - kics4net-scap-manager

- kics4net-scap-manager-view
- kics4net-scan-oval-manager
- kics4net-scheduler
- kics4net-secrets
- kics4net-task-m
- kics4net-task-mv
- kics4net-telemetry-proxy
- kics4net-vault
- kics4net-websensor
- kics4net-webserver

Preparing for centralized installation of components

Before preparing computers for the installation of application components, make sure that the centralized installation requirements have been fulfilled.

To prepare computers for installation of application components:

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

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

2. Find out and save the following information about the computers:

   - Name and IP address of the computer that will perform Server functions.
   - IP addresses of the computers that will perform sensor functions.
   - Name or IP address and SSL port of the computer with Kaspersky Security Center.

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

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

To connect:

a. Enter the following command in the command line:

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

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

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

```
exit
```

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

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

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

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

6. If you want to connect to Kaspersky Security Center and Kaspersky Security Center Network Agent is not installed on the computer where you are installing the Server, copy the Network Agent installation package (klnagent64-<Network Agent version>.x86_64.rpm) to kics4net-release_<application version number>/linux-centos.

You can download the package for installing Kaspersky Security Center Network Agent on the Kaspersky Endpoint Security for Business applications download page. To download the package, open the **Kaspersky Security Center** section and look in the list of subsections to find the line **Version <latest version number> | Red Hat Enterprise Linux x64 | Network agent**. Then, in this subsection, select a supported version of Kaspersky Security Center Linux (after that, the line will display the corresponding version of Network Agent) and the localization language of Network Agent. To start downloading, click the **Download** button in this subsection.

Centralized installation of application components

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

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

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

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

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

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

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

   A language menu will be displayed on the screen.

3. Select your language.

   The selected language will be used for the centralized installation menu and Kaspersky Industrial CyberSecurity for Networks components. After the Server is installed, application components will use the language selected at this stage.

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

   The main centralized installation menu appears on the screen.

5. Perform the following actions:

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

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

   c. When installing the Server with sensors, select **Add sensor** in the menu to add sensor nodes.

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

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

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

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

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

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

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

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

Centralized installation of application components in non-interactive mode

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

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

To prepare a centralized installation settings file using the script:

1. Configure the centralized installation settings by completing steps 1–5 of the installation procedure.
2. Save the installation settings file by selecting **Save settings and exit without installing**.

   The installation settings file named inventory.json is saved in the /home/<user>/.config/kaspersky/kics4net-deploy/ folder (the application components will not be installed).
3. If necessary, copy the centralized installation settings file into a different folder.

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

To centrally install application components in non-interactive mode:

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

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

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

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

   - `-i <path to the installation settings file>` – indicates the full path and name of the centralized installation settings file. If the setting is not defined, the inventory.json file located in the /home/<user>/.config/kaspersky/kics4net-deploy/ folder is used.
   - `--enable-debug-grpc-server` – installs a debug gRPC server. This gRPC server is used for testing purposes and is not required for normal use of the application.

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

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

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

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

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

Centralized installation menu commands

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

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

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

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

The commands in the main menu are organized into groups.

Server installation management commands

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

- **Add Server** – adds a new node that will be assigned Server functions. This item is available if the Server has not yet been added. If you select this option, you need to specify the main settings for the Server when the following prompts appear:

  - **Enter the IP address of the node for installation** – defines the IP address to be used for connecting to the computer over the SSH protocol and installing the Server.

  - **Add the capability for application interaction with Kaspersky Security Center** – adds the functionality that allows the use of the Kaspersky Security Center Administration Server to receive a license key and download updates, and to relay events and the application state to Kaspersky Security Center. You do not have to add this functionality to relay events to other recipient systems.

    If the capability for application interaction with Kaspersky Security Center has been added, the Network Agent component of Kaspersky Security Center is installed when the application is installed. This requires that the kics4net-release_<application version>/linux-centos directory, created when preparing for centralized installation of components contain a Network Agent installation package.

The 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 sensor nodes.

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

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

  - **Enable hardware Watchdog** – enables the 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 the hardware Watchdog is enabled, specify its path under **Specify path to hardware Watchdog**.

  - **Disable hardware Watchdog** – disables the use of the hardware Watchdog.

  - **Add the capability for application interaction with Kaspersky Security Center** – adds the functionality enabling the application to interact with Kaspersky Security Center (unless already added). This menu item is equivalent to the **Add the capability for application interaction with Kaspersky Security Center** item in the **Add Server** menu.

  - **Remove the capability for application interaction with Kaspersky Security Center** – removes the functionality that allows the application to interact with Kaspersky Security Center.

  - **Enable time synchronization between Server and sensors** – enables automatic time synchronization between the Server and nodes (unless already enabled). This menu item is equivalent to the **Enable time synchronization between Server and sensors** item in the **Add Server** menu.

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

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

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

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

Sensor installation management commands

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

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

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

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

  - **Enable hardware Watchdog** – enables the 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 the hardware Watchdog is enabled, specify its path under **Specify path to hardware Watchdog**.

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

General installation commands

General installation menu commands include the following commands:

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

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

Installation menu exit commands

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

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

Reconfiguration and centralized reinstallation of application components

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

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

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

To centrally reinstall components of Kaspersky Industrial CyberSecurity for Networks:

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

   The main centralized installation menu appears on the screen.
3. Depending on the necessary result, perform the following actions:

   - Select **Change Server settings** in the menu to specify Server settings.

     You cannot change the IP address of the Server. To change the IP address, first remove the existing Server and then add it again with the new IP address by selecting **Add Server** in the menu (this option appears if a Server has not been added).

- If the Server was installed with sensors, select **Change sensor settings** in the menu to specify settings for the sensors.

  You cannot change the IP address of a previously added sensor. To change the IP address, first remove the existing sensor and then add it again with the new IP address by selecting **Add sensor** in the menu. You can also use this menu item to add new sensors.

- Select **Change the user running the installation** in the menu to specify the user name of the account with root privileges that will be used to centrally install the application components on computers. This account will be used on those nodes for which no additional account was specified when configuring advanced settings of the Server or sensors.

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

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

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

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

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

Centralized removal of application components

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

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

To centrally remove application components from individual nodes:

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

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

   The main centralized installation menu appears on the screen.

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

   - Select **Remove Server** in the menu 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.

   - Select **Remove sensor** in the menu to remove a sensor node. If multiple sensors have been added to the application, select the relevant node in the list of nodes with added sensors.

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

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

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

To completely remove the application:

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

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

   The main centralized installation menu appears on the screen.

3. Select **Remove Server** in the menu to remove a Server node.

4. If sensors have been added to the application, select **Remove sensor** in the menu to remove all sensor nodes one by one.

5. Select **Removal settings** in the menu to configure advanced settings for centralized removal. When this item is selected, the following prompts are displayed:

   - **Remove the application together with data (y/n)?** 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 (y/n)?** If you want to remove the Kaspersky Security Center Network Agent component, enter `y`. If you do not need to remove this component, enter `n`. This prompt is displayed if an installed Network Agent is detected.

6. Select **Save settings and start installation**.

7. In the `SSH password` and `BECOME password` prompts, enter the password of the user account performing the centralized removal.

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

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

Local installation and removal of application components

This section provides information on local installation and removal of application components using the following scripts:

- kics4net-install.sh is the script for local installation of an application component.

- kics4net-remove.sh is the script for local removal of an application component.

The scenario for local installation of application components consists of the following steps:

1. **Fulfilling the requirements for local installation**

   At this step, make sure that the local installation requirements have been fulfilled.

2. **Preparing for application installation**

   At this step, prepare the computers for local installation of Kaspersky Industrial CyberSecurity for Networks components.

3. **Local installation of application components**

   At this step, perform local installation of application components on all computers by using the kics4net-install.sh script. The application components local installation script can install only one of the components (Server or sensor) on a computer.

4. **Reinforcing the security of computers with application components installed**

   After installing Kaspersky Industrial CyberSecurity for Networks, you are advised to harden the security of the operating systems on computers that have application components installed. Security is hardened by using the kics4net-harden.sh local startup script, which is located on the computer that has the installed application component in the /opt/kaspersky/kics4net/sbin/ directory.

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

   If you need to use Kaspersky Security Center functions for working with Kaspersky Industrial CyberSecurity for Networks, install the Kaspersky Industrial CyberSecurity for Networks administration plug-in. The following administration plug-ins are provided:

   - Web management plug-in for Kaspersky Security Center Web Console - this plug-in is intended for use in Kaspersky Security Center Linux, as well as for advanced centralized control and single sign-on technology in Kaspersky Security Center Windows. Install this plug-in using one of the methods available in the Kaspersky Security Center Web Console interface.

   - Management plug-in for Administration Console based on Microsoft Management Console (MMC) - this plug-in is intended for use in Kaspersky Security Center Windows. Install this plug-in locally on the computer where the Kaspersky Security Center Administration Server is installed.

6. **Startup configuration of the application after Server installation**

   After installing the Server, complete the initial configuration in the web interface of Kaspersky Industrial CyberSecurity for Networks. After the initial configuration is completed, the web interface page will open in the normal operating mode of the application.

After installing the application components, prepare the application for operation.

Requirements for local installation of application components

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

- The computer meets the hardware and software requirements.
- The equipment, hardware, and software of the computers are compliant with all operational security recommendations.
- To ensure proper functioning of application components, use specially dedicated computers that only have software from the operating system installed.

If third-party applications are installed on computers, the performance of components of Kaspersky Industrial CyberSecurity for Networks may be reduced.

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

    - kics4net-report-renderer
    - kics4net-report-tc
    - kics4net-report-tcv
    - kics4net-responses-manager
    - kics4net-risk-oval-detector
    - kics4net-scap-manager
    - kics4net-scap-manager-view
    - kics4net-scan-oval-manager
    - kics4net-scheduler
    - kics4net-secrets
    - kics4net-task-m
    - kics4net-task-mv
    - kics4net-telemetry-proxy
    - kics4net-vault
    - kics4net-webserver
- If a sensor will be installed:
    - kics4net
    - kics4net-apm
    - kics4net-connectors
    - kics4net-connectors-launcher
    - kics4net-epp-proxy
    - kics4net-nats
    - kics4net-nats-server
    - kics4net-oval-facade
    - kics4net-telemetry-proxy
    - kics4net-websensor

Preparing for local installation of the Server or a sensor

Before preparing computers for installation of application components, make sure that the local installation requirements have been fulfilled.

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

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

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

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

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

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

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

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

4. If you want to connect to Kaspersky Security Center and Kaspersky Security Center Network Agent is not installed on the computer where you are installing the Server, copy the Network Agent installation package (klnagent64-<Network Agent version>.x86_64.rpm) to kics4net-release_<application version number>/linux-centos.

   You can download the package for installing Kaspersky Security Center Network Agent on the Kaspersky Endpoint Security for Business applications download page. To download the package, open the **Kaspersky Security Center** section and look in the list of subsections to find the line **Version <latest version number> | Red Hat Enterprise Linux x64 | Network agent**. Then, in this subsection, select a supported version of Kaspersky Security Center Linux (after that, the line will display the corresponding version of Network Agent) and the localization language of Network Agent. To start downloading, click the **Download** button in this subsection.

Using a script for local installation of application components

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

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

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

When installing the Server, the Kaspersky Security Center Network Agent component is automatically installed. This requires that the kics4net-release_<application version>/linux-centos directory, created when preparing for local installation of components contain a Network Agent installation package.

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

To locally install a Kaspersky Industrial CyberSecurity for Networks Server:

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

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

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

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

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

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

   `--product-language=<language>` defines the application localization language. The setting can take the following values:

   - `english`—English
   - `russian`—Russian
   - `chinese-simplified` – simplified Chinese (supported only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).

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

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

4. If the start command does not contain the `--product-language=<language>` parameter, the language for application components is selected as follows:

   - If no components are installed on the computer, then before the installation process a menu appears, where you need to specify the number of the desired language.
   - If the Server component is found installed on the computer, then, when reinstalling the component, the script uses the language selected for the previous installation.

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

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

To locally install a Kaspersky Industrial CyberSecurity for Networks sensor:

1. Log in to the system using the account credentials of a user account with root privileges that you want to use to run the local installation script.
2. Go to the folder with the unpacked files of scripts and packages for installing, verifying and removing application components, included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.
3. Enter the command for starting local installation of a sensor:

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

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

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

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

Using a script for local removal of application components

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

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

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

   - If you want to delete the installed component files and all data saved by the application in the system, enter the command:

     ```
     bash kics4net-remove.sh --full
     ```

   - If you only want to delete the installed component files, enter the command:

     ```
     bash kics4net-remove.sh
     ```

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

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

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. You can use one of the following scripts to harden the security:

- Application components centralized installation script kics4net-deploy-<application version number>.bundle.sh that was obtained when preparing for the centralized installation of components.
- security hardening local startup script kics4net-harden.sh, which is located on the computer that has the installed application component in the /opt/kaspersky/kics4net/sbin/ directory.

You can use the kics4net-deploy-<application version number>.bundle.sh script or the kics4net-harden.sh script to do the following:

- 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).

Centralized reinforcement of computers' security using the kics4net-deploy-<application version>.bundle.sh script:

Application components centralized installation script kics4net-deploy-<application version>.bundle.sh performs actions that harden the security on all computers that have application components installed.

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

To harden the security of computers after centralized installation of application components:

1. On the computer from which the installation was performed, go to the directory containing the unpacked files of scripts and packages for installing, verifying and removing application components that are included in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.
2. Enter the following command:

```
bash kics4net-deploy-<application version number>.bundle.sh --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 `BECOME password` prompts, enter the password for the user account that is running the centralized installation.

Wait for the script to finish. If it completes successfully, information is displayed about the actions performed on computers with application components installed.

Locally hardening the security of computers using the kics4net-harden.sh script

If you have not performed centralized hardening of computers, you can use the kics4net-harden.sh script to locally harden the security of the computers. The local hardening procedure must be performed on each computer that has an application component installed.

To harden the security of the computer after local installation of the application component:

1. On the computer where the application component is installed, log in to the system using the account credentials of a user with root privileges.
2. Go to the /opt/kaspersky/kics4net/sbin/ directory and enter the following command:

```
sudo bash kics4net-harden.sh <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.

Wait for the script to finish. If it completes successfully, information is displayed about the actions performed.

Configuring a firewall on Server and sensor nodes

After installing Kaspersky Industrial CyberSecurity for Networks, you are advised to check the availability of the necessary ports and protocols on computers that have the application Server and sensors installed. During the installation of these components, the application automatically creates the necessary exclusions in the operating system firewall rules for the main ports and protocols that are used. In some cases, you may need to open additional ports that are on the list of ports and protocols that can be used in Kaspersky Industrial CyberSecurity for Networks.

To check and fine-tune the defined exclusions in the firewall rules on the node:

1. On the computer where the application component is installed, log in to the system using the account credentials of a user with root privileges.

2. Open the operating system console and enter the following command:

   ```
   sudo firewall-cmd --list-all
   ```

3. Check the list of port and protocol exclusions displayed in the `ports` line.

   By default, the list contains exclusions for the main ports and protocols that are used. You need to check whether this list contains the necessary ports that are used for specific functionality of Kaspersky Industrial CyberSecurity for Networks. For example, to use the functionality for interacting with Kaspersky Security Center, the firewall on the Server computer must at least have exceptions defined for TCP port 13000 and UDP port 15000.

4. Add exclusions for the necessary ports and protocols. To do so, sequentially specify the data by using the following command:

   ```
   sudo firewall-cmd --zone=public --permanent --add-port=<port number>/<protocol>
   ```

   Example

   ```
   sudo firewall-cmd --zone=public --permanent --add-port=15000/udp --add-port=13000/tcp
   ```

5. Restart the firewall service. To do so, enter the following command:

   ```
   sudo firewall-cmd --reload
   ```

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

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

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

  The management plug-in for the MMC-based Administration Console must be installed locally on the computer where the Kaspersky Security Center Administration Server is installed. To install, you need to use a file from the Kaspersky Industrial CyberSecurity for Networks kit.

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

  You must install the web plug-in on the computer that has the Kaspersky Security Center Web Console installed. The web plug-in functions are available to all administrators who have access to the Kaspersky Security Center Web Console through a browser. You can update the installed version of the web plug-in after new versions of Kaspersky applications are released.

Installing the management plug-in for the MMC-based Administration Console

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

- Using the Setup Wizard
- From the command line

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

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

To install the administration plug-in using the Wizard:

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

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

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

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

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

1. On the computer where the Kaspersky Security Center Administration Server is installed, open the command line interface.
2. Go to the folder that contains the file named kics4net-sc-plugin_<plug-in version number>_<localization code>.msi.

3. Enter the following command in the command line:

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

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

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

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

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

Installing the administration web plug-in for the Kaspersky Security Center Web Console

You can install the web plug-in by using any of the following methods:

- Install the web plug-in from the list of available distribution packages in the Kaspersky Security Center Web Console.

  To install the web plug-in, select the web plug-in distribution package in the Kaspersky Security Center Web Console interface: **Console settings → Web plug-ins**. The list of available distribution packages is updated automatically after new versions of Kaspersky applications are released.

- Download the distribution package from the list of available distribution packages, plug-ins and patches for Kaspersky Security Center.

  To install the web plug-in, select the web plug-in distribution package in the Kaspersky Security Center Web Console interface: **Operations → Kaspersky applications → Current application versions**. The list of available distribution packages is updated automatically after new versions of Kaspersky applications are released.

- Install the web plug-in by using the file provided in the Kaspersky Industrial CyberSecurity for Networks distribution kit (see below).

To install the web plug-in using the file provided in the application distribution kit, you need to copy the kics4net-web-ksc-plugin_<web plug-in version number>.zip file to the computer that has the Kaspersky Security Center Web Console server installed. You can copy the file from the directory containing the unpacked files of the kics4net-release_<application version number>.tar.gz archive to the computer where preparations for application installation were completed. After unpacking the archive, the file for installing the web plug-in is located in the kics4net-release_<application version number>/sc_plugin subdirectory.

To install the administration web plug-in for the Kaspersky Security Center Web Console using the file from the application distribution kit:

1. On the Kaspersky Security Center Web Console server computer, unpack the copied kics4net-web-ksc-plugin_<web plug-in version number>.zip file.
2. In the Kaspersky Security Center Web Console interface, go to **Console settings** → **Web plug-ins** and click the button for adding a web plug-in from a file.
3. Specify the files from the unpacked archive directory in sequence: plugin.zip and signature.txt.
4. In the opened window, verify the success of the operations completed during installation of the web plug-in and close the window.

   The **Kaspersky Industrial CyberSecurity for Networks** web plug-in appears in the list of installed web plug-ins.

Startup configuration of the application after Server installation

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

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

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. Use the IP address of the Server computer for the connection.
2. Select **Startup configuration**.
3. Select the localization language for the program's web interface.

   Going forward, you can select another web interface language in normal mode.
4. In the **Administrator account** settings group, define the user account name and password for the first application user. The Administrator role will be assigned to this user. This user does not have to be registered as an operating system account on the Server computer or other computer.

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

   The password must meet the following requirements:

   - Must contain between 8 and 256 ASCII characters.
   - Must contain one or more uppercase letters of the English alphabet.
   - Must contain one or more lowercase letters of the Latin alphabet.
   - Must contain one or more numerals.
   - Must contain no more than three consecutive repeated characters.

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

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

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

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

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

8. Click **Continue**.

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

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

Certificates used in Kaspersky Industrial CyberSecurity for Networks

To ensure the security of connections, Kaspersky Industrial CyberSecurity for Networks uses digital certificates. The application automatically creates the necessary certificates during installation (centralized or local) and when adding objects whose interaction requires certificates. All automatically generated certificates are self-signed on the application Server side.

About the utilized certificates

To ensure the security of connections, Kaspersky Industrial CyberSecurity for Networks uses the following certificates:

- Main Server certificate and application service certificates (including the web server service certificate on the application sensor)
- Certificate for connecting to the Server through the web interface
- Certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API

- Certificates for connecting connectors.
- Certificates for connections with the Endpoint Agent software components.

You can replace some automatically generated certificates with digital certificates that were issued by trusted certification centers. The replacement procedure is performed when the following certificates are updated:

- Certificate for connecting to the Server through the web interface
- Certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API

Updating the application using the data migration script does not provide the capability to save the certificates currently in use. When you perform this procedure, the application creates new certificates just like after a normal installation. Therefore, previously created connectors stop working in the application. To restore their operation, you need to update the certificates for connecting the connectors.

Updating SSL connection certificates

Automatically generated certificates are given an expiration date that exceeds the life cycle of the current version of the application (see the Application life cycle page). However, to ensure secure operation of the application, it is not recommended to use the same certificates for a long time. The automatically generated certificates should be replaced with new ones at regular intervals by updating the certificates.

You are advised to update the certificates being used in the application 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.

Update procedures may be performed differently depending on the application scope of the certificates being used. There are also differences in the subsequent steps to be performed after updating certificates.

Updating the main certificate of the Kaspersky Industrial CyberSecurity for Networks Server

The main certificate of the Application Server is used for connections between nodes of Kaspersky Industrial CyberSecurity for Networks. Along with other certificates, this certificate is automatically generated by the application during its installation. Replacing this certificate during its update affects the validity of most other certificates that are used in the application and depend on the main certificate. Therefore, when performing the update procedure for the main Server certificate in the application, the following certificates must also be updated:

- Application service certificates (including the web server service certificate on the application sensor): updated automatically.
- Certificate for connecting to the Server through the web interface: updated automatically.

- Certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API: updated automatically.
- Certificates for connecting connectors: updated manually.

When the main Server certificate is replaced, the old certificates of the application sensors become invalid. This leads to termination of the connections between the sensors and the Server. To resume connections as part of the certificate renewal procedure, you will need to re-add and reconnect all sensors. You will also need to update the certificates used for connecting connectors.

After the update of the main Server certificate is completed, the application uses self-signed certificates to connect to the Server through the web interface and to connect via the Kaspersky Industrial CyberSecurity for Networks API. To replace these certificates with digital certificates that were issued by trusted certification centers, you must additionally complete the steps to update the certificate for connecting to the Server through the web interface and update the certificate for connecting to the Server via the Kaspersky Industrial CyberSecurity for Networks API.

To update the main Server certificate and its dependent certificates:

1. On the Server computer, go to the /opt/kaspersky/kics4net/sbin/ folder and enter the command to launch the script for local certificate update:

   ```
   sudo bash kics4net-update-certs.sh
   ```

2. Wait for the script to finish.
3. On each computer that has an installed sensor, reset the sensor to its initial state. To do so, go to the /opt/kaspersky/kics4net/sbin/ directory and enter the command to run the script for locally switching the node to its initial state:

   ```
   sudo bash kics4net-reset-to-defaults.sh
   ```

4. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator account and re-add and connect the sensors.
5. If connectors have been added to the application, update the certificates to connect them.

Updating the certificate for connecting to the Server through the web interface

A certificate for connecting to the application Server through the web interface is automatically created by the application during its installation, and when updating the main Server certificate or when updating the application using the data migration script. The automatically generated certificate is self-signed on the application Server side.

It is not recommended to constantly use a self-signed certificate to connect to the Server. You can use such a certificate temporarily (for example, during test operation of Kaspersky Industrial CyberSecurity for Networks). For permanent use, it is recommended to replace this certificate with another one that was issued by a trusted certification center.

The application supports downloading certificates from PFX files. You can obtain the trusted certificate file with the help of the system administrator of your organization.

To update the certificate for connecting to the Server through the web interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection servers**.
3. On the **Web server** tab, specify the local path to the certificate file by using the **Browse** button.
4. In the **Certificate access password** field, enter the certificate access password.
5. Click **Apply**.
6. In the request window, confirm that you want to apply the specified parameters and connect to the Server.

Updating the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API

A certificate for connecting to the application Server via the Kaspersky Industrial CyberSecurity for Networks API is automatically created by the application during its installation, and when updating the main Server certificate or when updating the application using the data migration script. The automatically generated certificate is self-signed on the application Server side.

It is not recommended to constantly use a self-signed certificate to connect to the Server. You can use such a certificate temporarily (for example, during test operation of Kaspersky Industrial CyberSecurity for Networks). For permanent use, it is recommended to replace this certificate with another one that was issued by a trusted certification center.

The application supports downloading certificates from PFX files. You can obtain the trusted certificate file with the help of the system administrator of your organization.

When the certificate for connecting to the Server via the Kaspersky Industrial CyberSecurity for Networks API is replaced, the old certificates for connecting the connectors become invalid. This leads to termination of the connections between the connectors and the Server. To resume the connections, you will need to update the certificates of the connectors.

To update the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection servers**.
3. On the **REST API server** tab, specify the local path to the certificate file by using the **Browse** button.
4. In the **Certificate access password** field, enter the certificate access password.
5. Click **Apply**.
6. In the prompt window, confirm that you want to apply the specified parameters.
7. If connectors have been added to the application, update the certificates to connect them.

Updating certificates for connecting connectors

A certificate for connecting each connector is automatically generated by the application when this connector is added to the application. Certificates of all connectors are valid until one of the following procedures is completed:

- Updating the main certificate of the Kaspersky Industrial CyberSecurity for Networks Server
- Updating the certificate for connecting to the Server through the Kaspersky Industrial CyberSecurity for Networks API
- Updating Kaspersky Industrial CyberSecurity for Networks or restoring from a backup copy using a data migration script

After completing any of the listed procedures, you need to update the certificates of all connectors that were added to the application. In addition, you may be required to update the connector certificates regardless of the listed procedures in accordance with the certificate update recommendations.

The steps for updating certificates for each connector depend on whether the connector is managed or unmanaged. For unmanaged connectors, the certificate update procedure affects only the running services of connectors. These connectors do not need to be removed to update their certificates. When updating certificates of managed connectors, you will need to remove these connectors from the application and add them again.

Generic and **KUMA** connectors are always unmanaged. Connectors of other types that are built into the application can be either managed or unmanaged. When creating such connectors, the user can enable the mode for ignoring the functions of a managed connector, which makes the created connector unmanaged. In the connectors table, the managed connector indicator is displayed for each connector in the **Manageable** column.

To update the certificate for connecting an unmanaged connector:

1. Complete the procedure for creating a new communication data package for the connector.

2. Register a new certificate in the connector service. To do so, complete the following actions on the connector deployment node (a node with the installed Server or sensor):

   - If the certificate for a **Syslog**, **SIEM**, **Generic**, **Email** or **Cisco Switch** connector has been updated, go to the /opt/kaspersky/kics4net-connectors/libexec/ directory and enter the following command to start the script for working with connectors:

     ```
     sudo python3 default_connectors_registrar.py update
     ```

     When prompted by the script to provide connector data, enter the name of the connector, the path to the communication data package, and the connector certificate access password.

     Wait for the script to finish and enter the command to restart the connector service:

     ```
     sudo systemctl restart kics4net-connectors@{<connector name>}
     ```

   - If the certificate for an **Active poll** connector has been updated, go to the /opt/kaspersky/kics4net-apm/src/ directory and enter the following command to run the script for working with the connector:

     ```
     sudo python3 register.py -p "<full path to the communication data package>"
     ```

     Wait for the script to finish and enter the command to restart the active polling connector service:

     ```
     sudo systemctl restart kics4net-apm
     ```

To update the certificate for connecting a managed connector:

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

2. Select **Settings** → **Connectors** and select the necessary connector on the **Connectors** tab.

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

3. Check the currently defined connector settings and take the steps to restore the necessary settings in the new connector after removing this connector.

   For example, you can use any text editor to save the name and public key of a switch for a **Cisco Switch** connector or the addresses and specific templates for an **Email** connector. All text content of the details area can be selected with your mouse and copied using the tools of the browser and operating system (via the context menu or by using the keyboard shortcuts for working with the clipboard).

4. Delete the connector.

5. Re-add the same connector to the application.

Updating certificates for connections with the Endpoint Agent software components

In Kaspersky Industrial CyberSecurity for Networks, certificates for connections with Endpoint Agent software components are used by integration servers. Certificates are required for the integration server if this server is running in TCP mode. Certificates for the integration server and its clients are issued by the application Server. These certificates may need to be updated according to the recommendations on updating certificates.

To update the certificates of the integration server:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection servers**.
3. On the **Integration servers** tab, select the server for whose clients you want to update the utilized certificates.

   The details area appears in the right part of the web interface window.
4. To issue a new certificate for the integration server, click the **Reissue certificate** button.

   After the integration server certificate is replaced, its old certificate becomes invalid.
5. To issue new certificates for clients of the integration server, complete the following actions in the **Certificates for clients (TCP mode)** section:

   a. Delete the old certificates by using the × icon that is located on the right of the field containing the certificate fingerprint.

   b. Add new certificates by using the **Create new certificate** button.
6. Click **Save**.
7. Create a communication data package and download it to client computers.

Updating using data migration script

You can upgrade a previous version of Kaspersky Industrial CyberSecurity for Networks by using the kics4net-backup.sh data migration script from the distribution kit of the current (new) version of the application. The capability to upgrade to the current version using the kics4net-backup.sh script is supported for application version 4.0 or later.

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

- Security policy
- Data on the state and/or operating modes of technologies and methods
- Settings for updating application modules and databases
- Information about an added license key

- Audit entries
- Application messages
- Vulnerability risks
- Registered events
- Saved traffic for events
- Network map data
- Registered network sessions with saved protocol attributes
- Data on executable files

You can also use the kics4net-backup.sh script to back up the data of the current application version. In addition to getting the data listed above, the script lets you additionally back up the following data on the node computer where the application component is installed:

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

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

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

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

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

   1. On the computer that has the previous version of the application components installed, copy the archive named kics4net-release_<application version number>.tar.gz from the distribution kit of the current (new) application version into a directory of your choice.
   2. Go to the folder containing the copied archive and enter the following command to unpack it:

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

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

4. Run the kics4net-backup.sh script:

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

```
sudo bash kics4net-backup.sh -b -p <path to the backup file> <optional settings>
```

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

```
sudo bash kics4net-backup.sh -s -p <path to the backup file> <optional settings>
```

where:

- `-b` is a setting that enables logging Server data to the backup file (mandatory setting when the Server is running on the computer).
- `-p` is a setting indicating the full path and name of the created backup file (required setting).
- `-s` is a setting that enables logging sensor data to the backup file (mandatory setting when the sensor is running on the computer).
- `<optional settings>` refers to one or more of the optional settings listed below.

You can use the following optional settings in the command for running the script to create a backup file:

- `-t` is a setting for disabling retention of traffic (if this setting is not specified, traffic is saved).
- `-e` is a setting for disabling retention of registered events (if the setting is not specified, events are saved). You can specify this setting only when creating a backup copy of data on the Server computer.
- `-n` is a setting for disabling retention of network map data (if the setting is not specified, network map data is saved). You can specify this setting only when creating a backup copy of data on the Server computer.
- `-x` is a setting for disabling retention of data related to executable files (if the setting is not specified, data on executable files is saved). You can specify this setting only when creating a backup copy of data on the Server computer.
- `-a` is a setting for disabling retention of protocol attributes in registered network sessions (if the setting is not specified, protocol attributes are saved). You can specify this setting only when creating a backup copy of data on the Server computer.
- `-d` is a setting that stops the application services (if this setting is not specified, the application services are started after the script finishes).

An optional setting for the script run command is the `-f` setting, which is designed to create a backup copy of the data of the current version of the application and save all available data of the node. If this setting is specified, the saved data can be fully loaded only on the same node and in the same version of the application (including the same build number). When the `-f` parameter is used, the application saves traffic (unless traffic retention is disabled by using the `-t` parameter), events, network map data, data on executable files, protocol attributes in network sessions, and the following data to the backup file: node deployment parameters (including parameters of monitoring points and settings for storing data on nodes), a list of application users, settings of connectors, settings of connector types, settings of connection servers, settings for interaction with Kaspersky Security Center, data on installed application module and database updates, log levels for logging the activity of processes on nodes, and settings of widgets used for online system monitoring.

Example

```
sudo bash kics4net-backup.sh -b -p ./old_kics4net_data -t
```

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

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

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

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

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

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

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

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

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

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

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

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

   After installing the components, you need to partially prepare the application for operation by completing the following steps:

   - Initial configuration of the application
   - Adding and connecting sensors
   - Adding monitoring points
   - Adding application users

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

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

To download data from the created backup files, perform the following steps on each computer where the application component is installed:

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

2. Run the kics4net-backup.sh script:

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

     ```
     sudo bash kics4net-backup.sh -r -p <path to the backup file> <optional setting>
     ```

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

     ```
     sudo bash kics4net-backup.sh -l -p <path to the backup file> <optional setting>
     ```

   where:

   - `-r` is a setting that enables reading and downloading of data from the Server backup file (mandatory setting when running on the Server computer).
   - `-p` is a setting indicating the full path and name of the backup file (required setting).
   - `-l` is a setting that enables reading and downloading of data from the sensor backup file (mandatory setting when running on the sensor computer).
   - `<optional setting>` – `-d` is a setting that stops the application services (if this setting is not specified, the application services are started after the script finishes).

   An optional setting for the script run command is the `-f` parameter, which is intended to restore all available node data from the backup copy of the data of the current version of the application (if the backup copy was obtained at stage 1 of this scenario using the `-f` setting). However, all data can be fully restored only when loaded from a backup copy on the same node where this data was saved and in the same version of the application (including the same build number).

The additional run command settings `--restore-database` and `--restore-clickhouse-database` are provided for specific scenarios for using the kics4net-backup.sh script. These settings are intended for restoring only the corresponding Server databases from a backup file. These settings are not used in the scenario for upgrading from a previous version of the application. The `-r` setting (see above) is intended for reading and loading data from the Server backup file, including data for restoring the databases.

Example

```
sudo bash kics4net-backup.sh -r -p ./old_kics4net_data
```

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

After loading data from backups on all nodes, connect to the Server via the web interface and check the node deployment settings under **Settings** → **Deployment**. Add sensors if necessary.

If the connectors are restored in the application, update the certificates to connect them.

Installing an updated application version with a patch

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

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

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

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

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

- Security policy
- Data on the state and/or operating modes of technologies and methods
- Settings for updating application modules and databases
- Information about an added license key
- Audit entries
- Application messages
- Vulnerability risks
- Registered events
- Saved traffic for events
- Network map data, including network sessions with saved protocol attributes
- Traffic dump files
- Node deployment settings, including monitoring point settings and settings of data storage on the nodes
- List of program users
- Connector settings

- Connector type settings
- Connection server parameters
- Settings for interaction with Kaspersky Security Center
- Data on installed updates of databases and application modules
- Logging levels for processes running on the nodes
- Settings of live system monitoring widgets

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

You can use the kics4net-install-patch.sh script to install the updated application files for the current version or any version starting with 4.1, provided that the updated application files are compatible with the installed operating system and Kaspersky Industrial CyberSecurity for Networks versions.

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

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

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

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

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

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

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

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

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

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

To prepare the directory:

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

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

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

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

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

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

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

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

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

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

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

where:

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

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

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

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

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

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

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

Example

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

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

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

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. Use the IP address of the Server computer for the connection.
2. Select **About** and view the version of the application installed on the Server.
3. Select **Startup configuration**.
4. Please read the terms of the End User License Agreement and the Privacy Policy. To do this, open each document by clicking the corresponding links in the names of the following check boxes: **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement** and **I am aware and agree that my data will be handled and transmitted (including to third countries) as described in the** in the **Privacy Policy. I confirm that I have fully read and understand the terms of the Privacy Policy**.
5. If you fully agree to the terms of the End User License Agreement and the Privacy Policy, select both check boxes.

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

6. Click **Continue**.

Starting and stopping the application

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

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

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

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

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

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

Connecting to the Server through the web interface

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

To connect to the Kaspersky Industrial CyberSecurity for Networks Server:

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

   where:

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

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

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

   Be careful when entering the user name and password. If the user password is entered incorrectly multiple times in a row, a user with the Administrator role will receive a notification in the web interface. Subsequent repeated attempts at entering an invalid password may trigger an automatic 30-minute lockout that prevents connection to the Server through the web interface.

   If the administrator has enabled a mandatory password change for the account the first time the user connects to the application after the account has been created and/or after the administrator has changed the password, the **New password** and **Repeat new password** fields will be displayed on the account credentials entry page to change the application user's password.

3. When the fields for changing the application user's password appear, enter the new password and click the **Log in** button.

   The new password must satisfy the conditions listed on the account credentials entry page. The conditions you fulfill are automatically marked while you are entering your password.

After correctly entering the user name and password or changing the user password when connecting to the application, the Kaspersky Industrial CyberSecurity for Networks Server web interface page will open in your browser window. The name of the browser bookmark for the web interface page will show the Server name that was defined during startup configuration of the application after installation.

A Server connection session has a time limit. A session remains open for 10 hours by default (if necessary, you can change the session time limit by running the kics4net-params script). If 10 hours have passed since the connection was established, the current page of the application web interface switches to the page for entering account credentials. If this happens, to continue working you will need to re-enter your application user name and password.

Terminating a Server connection session through the web interface

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

If you close the browser window without first finishing the connection session, the session will remain active. A session remains active for 10 hours by default. During this time, the application can grant access to the web interface of the Kaspersky Industrial CyberSecurity for Networks Server without prompting for user account credentials, provided that the connection is used by the same computer, browser, and operating system account. If necessary, you can change the session time limit by running the kics4net-params script.

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

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

The browser window shows the page for entering account credentials.

Connecting to a sensor through the web interface

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

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

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

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

To connect to a Kaspersky Industrial CyberSecurity for Networks sensor:

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

where:

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

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

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

Application interface

This section describes the primary application interface elements.

You can connect to the application components (Server and sensors) via the web interface. You must use supported browsers for these connections. After connecting to an application component, a page containing interface elements is loaded in the browser window. The specific interface elements that you see will depend on which component you are connected to, the specific state of this component, and other factors.

On the Kaspersky Industrial CyberSecurity for Networks Server web interface page, the interface elements are divided into different functional sections. The sections are intended for configuring the application, managing its operation, and viewing data. You can select the relevant sections by using the menu of the web interface. The number of sections available for selection depends on the application mode and on the role of the user account.

On the Kaspersky Industrial CyberSecurity for Networks sensor web interface page, only two sections are always used to group interface elements. In these sections, you can get information about the connection between the sensor and the Server, and you can view brief information about the application.

About the Kaspersky Industrial CyberSecurity for Networks Server web interface

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

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

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

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

About the Kaspersky Industrial CyberSecurity for Networks sensor web interface

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

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

- Before connecting the sensor to the Server – management elements for selecting a communication data package and/or data for automatically connecting the sensor over the network.
- After connecting the sensor to the Server – data on the Server and sensor (including the capability to proceed to the Server web interface page) and the connection state.

Server web interface menu during startup configuration of the application

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

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

The web interface menu contains the following items:

- – expands and collapses the menu. If the menu is collapsed, the items are displayed without text descriptions.
- – opens the **Startup configuration** section.
- – opens a section containing brief information about the application.

Server web interface menu during normal operation of the application

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

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

The web interface menu contains the following items:

- – expands and collapses the menu. If the menu is collapsed, the items are displayed without text descriptions.
- – opens a list of notifications regarding application operating issues. The availability of notifications is indicated by an icon whose color corresponds to the status of the notifications.
- – opens a list of background operations. This list contains information about operations that take a long time (for example, creating a file when exporting a large number of events). The number of active background operations and their progress status are indicated by an icon. The icon is colored red if there are operations that resulted in errors.
- – opens the **Dashboard** section.
- – opens the **Assets** section.
- – opens the **Network map** section.
- – opens the **Events** section.
- – opens the **Reports** section.
- – opens the **Process control** section.
- – opens the **Allow rules** section.
- – opens the **Detection rules** section.
- – opens the **Risks** section.
- – opens the **Security audit** 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. When the menu is maximized, the **Not all protection services are running** notification is displayed. Clicking this icon or text opens a window containing information about disabled protection functions.
- **Connection server** – displays the name of the Server to which the connection was established (the name defined during startup configuration of the application after installation).

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

  - **Language** – lets you select the language of the application web interface.

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

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

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

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

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

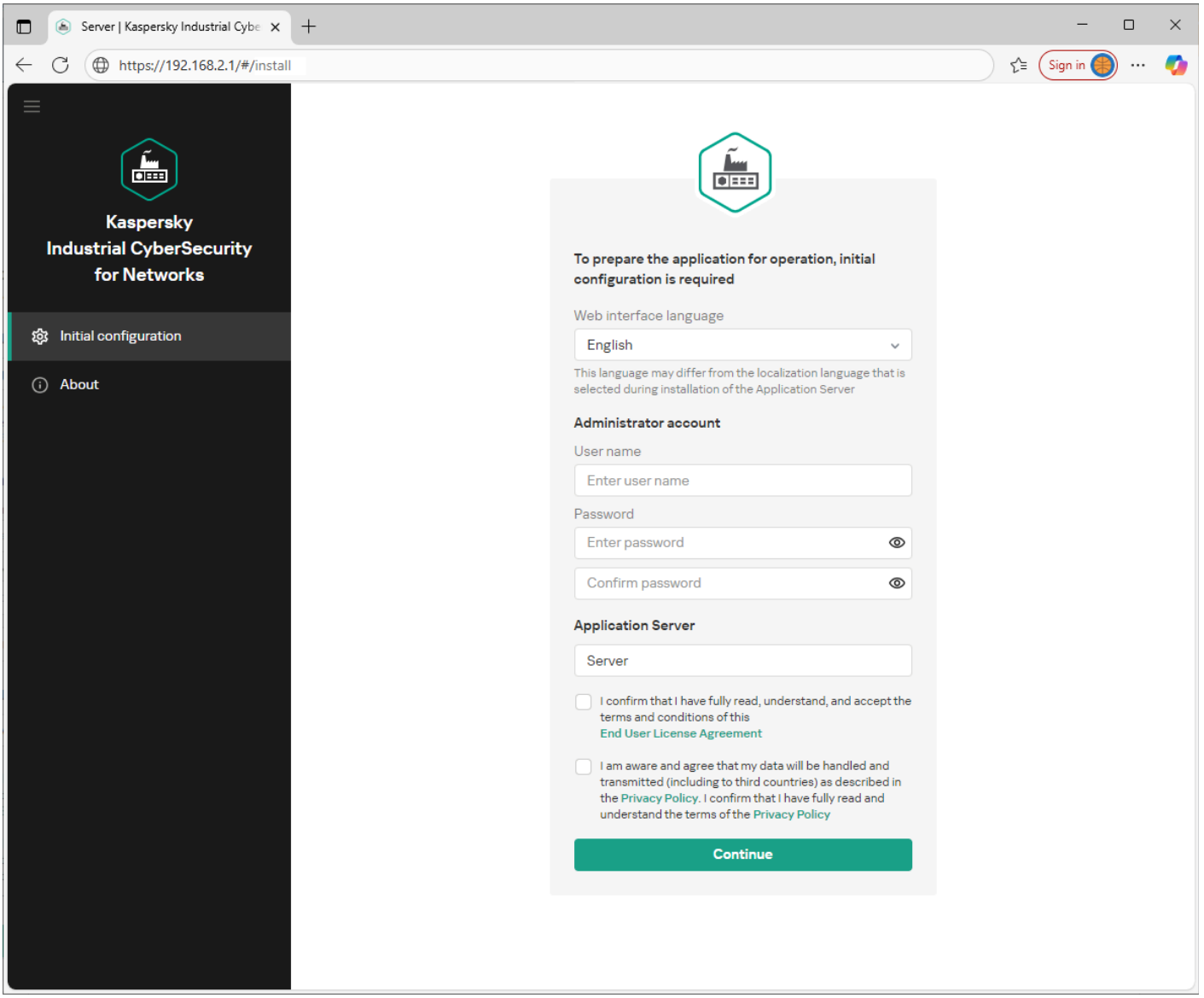
    - **Change password** – opens the window for changing the password of the current user.

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

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

Initial configuration section

In the **Startup configuration** section of the Server web interface (see the figure below), you can specify the main Application Server settings that are required for starting the application after it is installed.

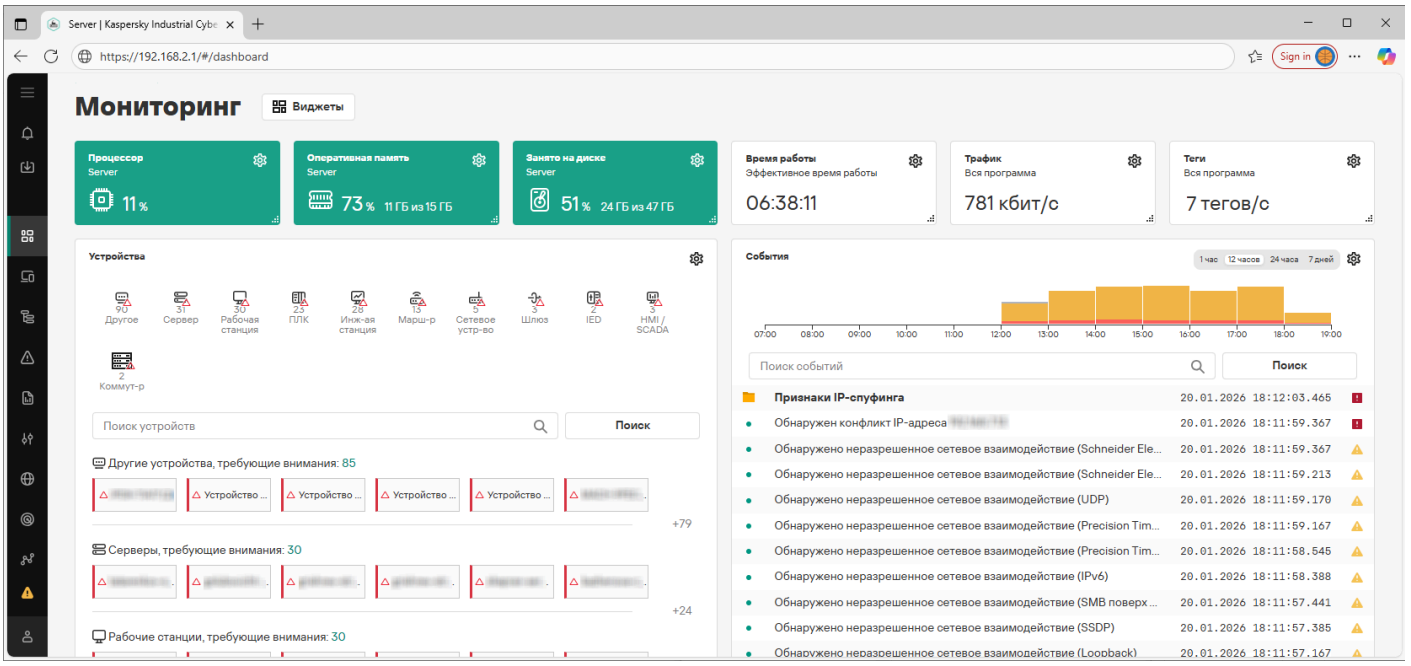


Startup configuration section

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

Dashboard section

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



Dashboard section

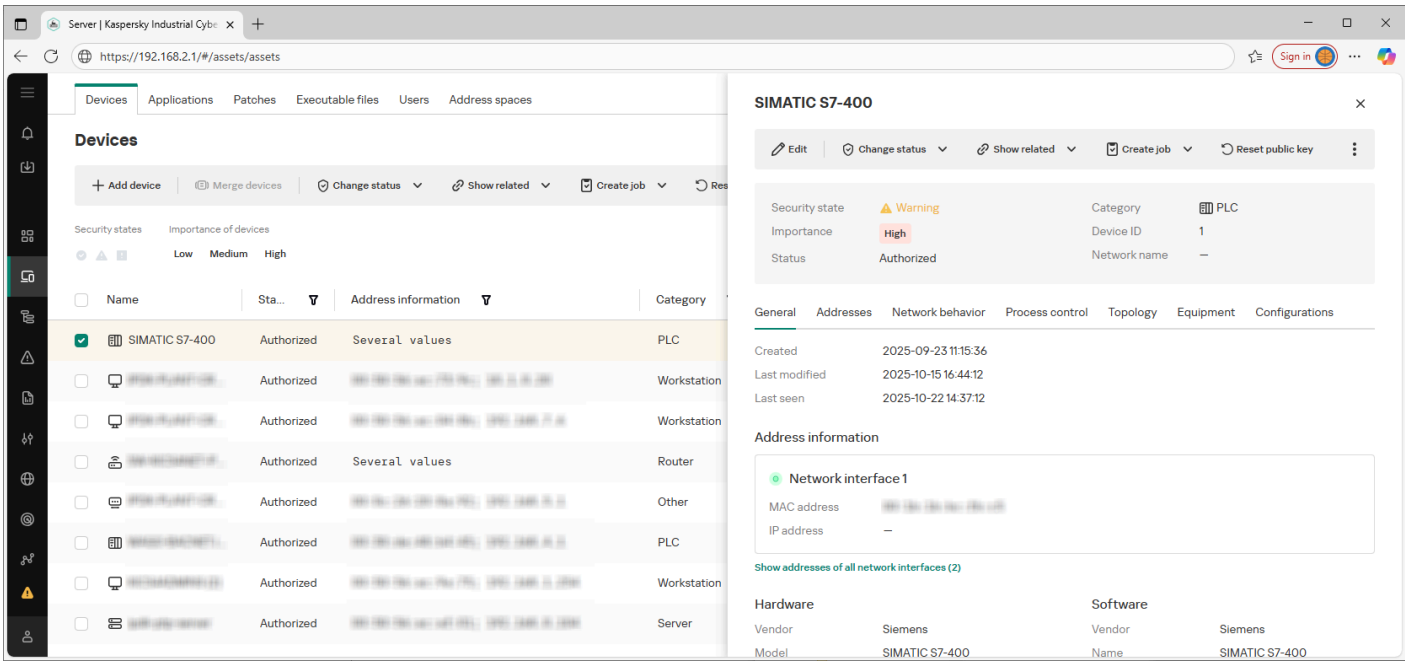
You can watch the tutorial video (see below) to familiarize yourself with the functionality.

https://www.youtube.com/watch?v=zxP9OniGjkM

Dashboard overview

Assets section

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



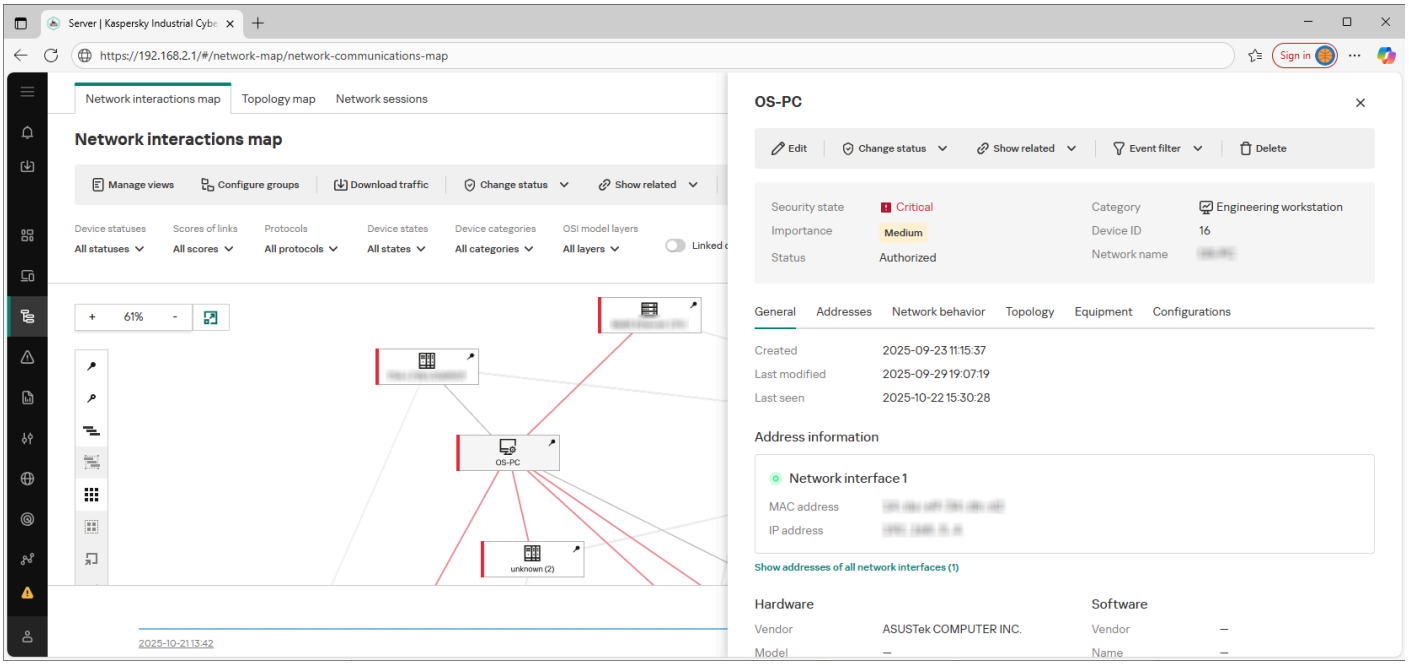
Assets section

The **Assets** section contains a tab with a table of devices, tabs with tables of main objects on devices (applications, patches, executable files, and users), and a tab with information about address spaces.

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

Network map section

In the **Network map** section of the Application Server web interface (see the figure below), you can view information about interactions on the network map and in the network sessions table, as well as generate a topology map.



Network map section

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

When you select an object, the details area opens in the right part of the section. The details area contains information about the selected object and the tools for managing it.

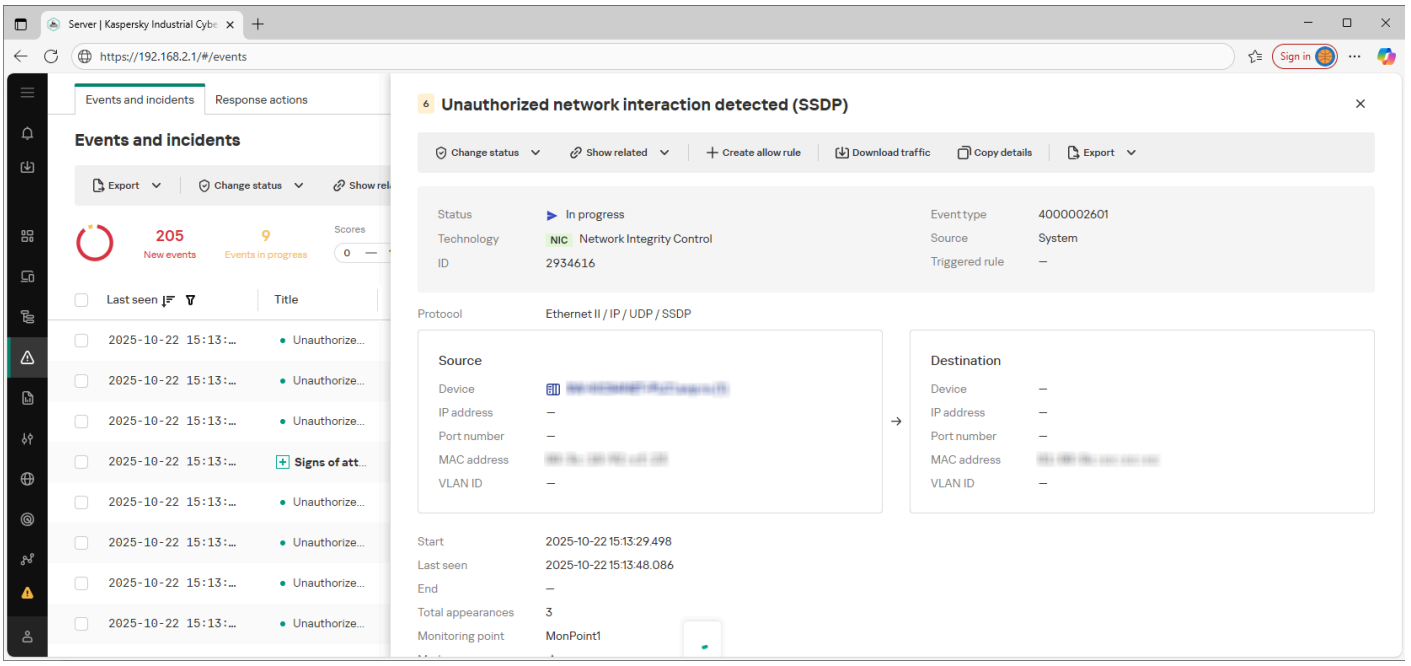
You can watch the tutorial video (see below) to familiarize yourself with the functionality.

https://www.youtube.com/watch?v=5uPjUMi5Qjo

Network inventory

Events section

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



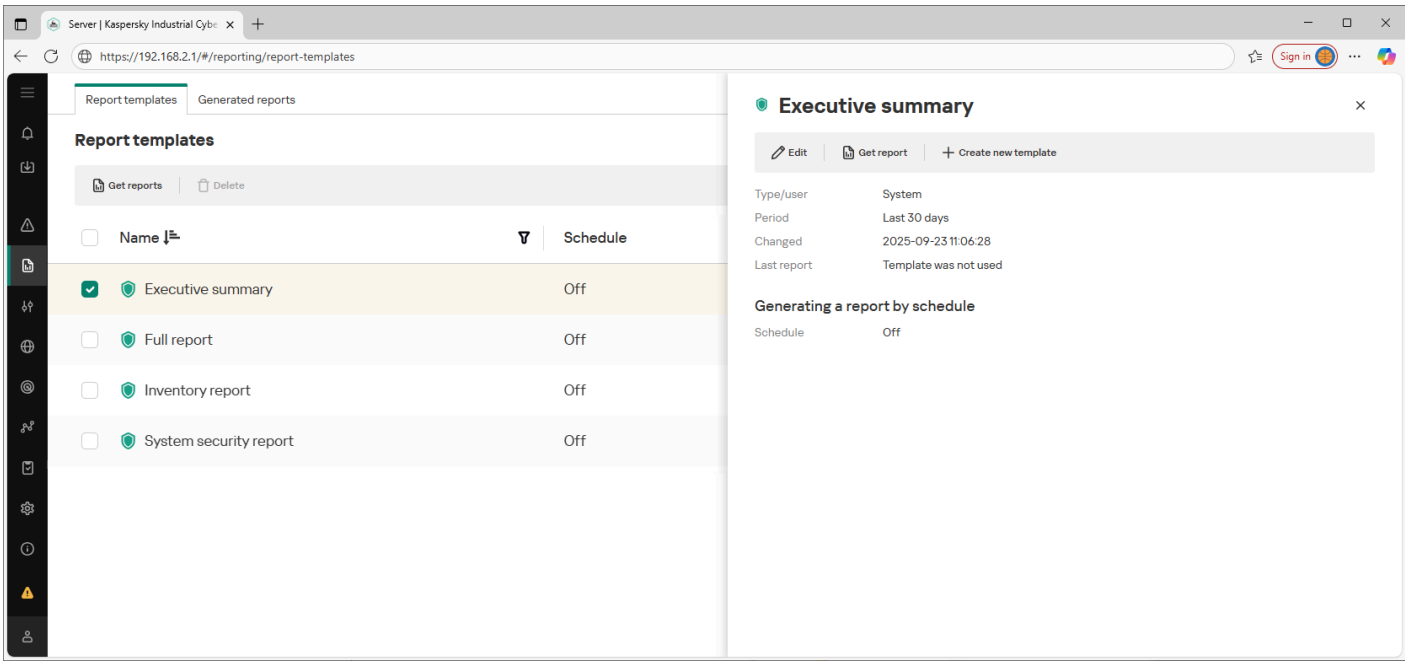
Events section

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

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

Reports section

In the **Reports** section of the Application Server web interface (see the figure below), you can view the generated reports and report templates, as well as manage reports and report templates.



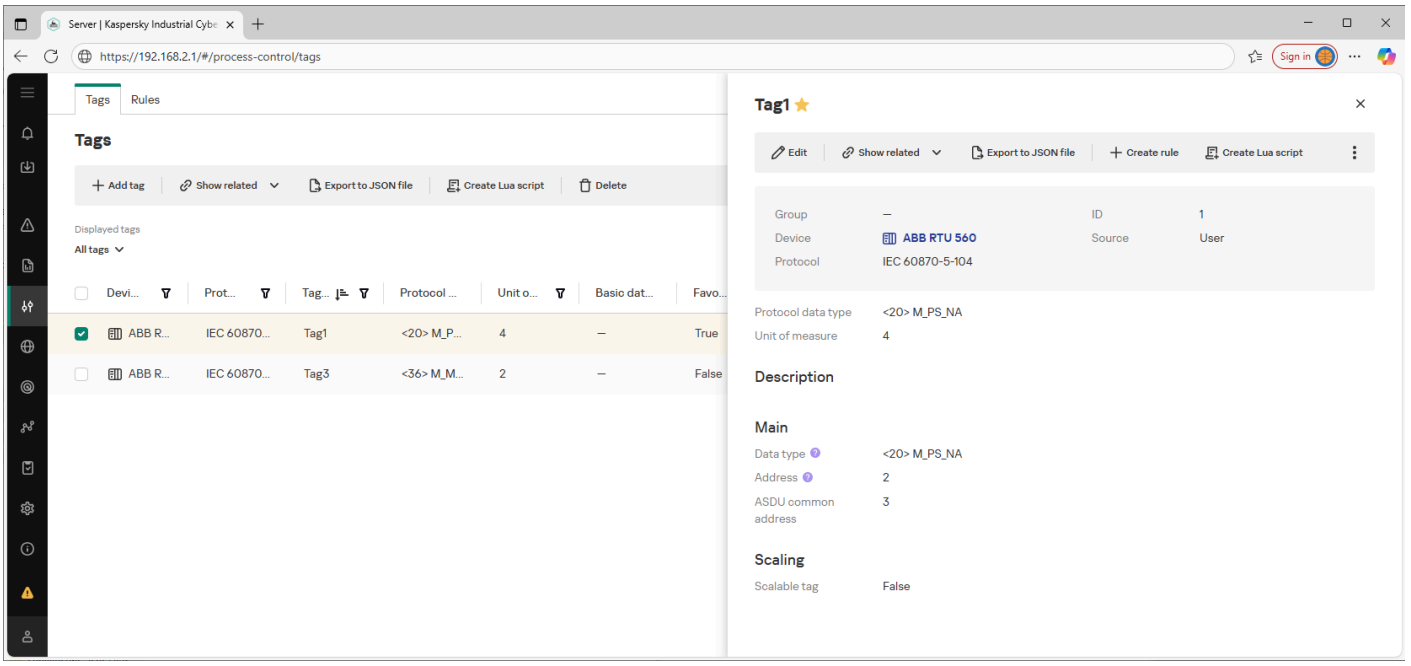
Reports section

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

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

Process control section

In the **Process control** section of the Application Server web interface (see the figure below), you can view the values of the industrial process parameters (tags), as well as configure tags and rules for the process control.



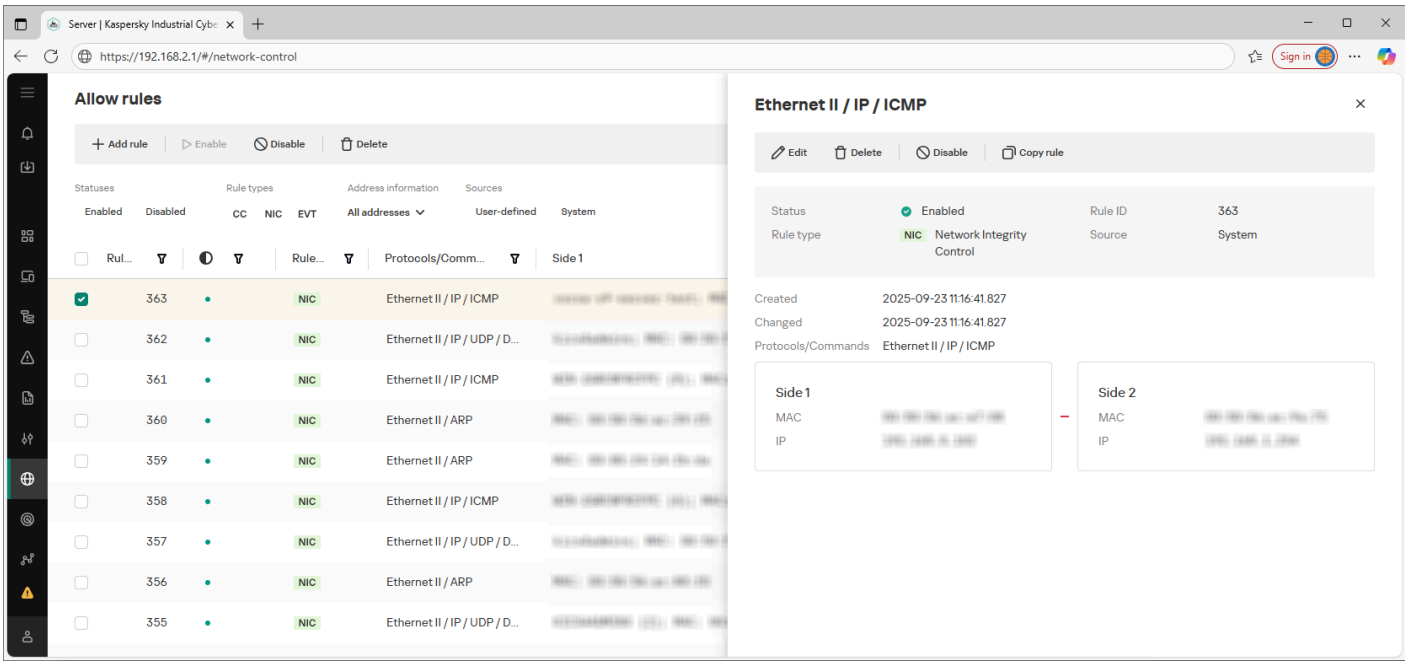
Process control section

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

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

Allow rules section

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



Allow rules section

The **Allow rules** section contains a table of allow rules.

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

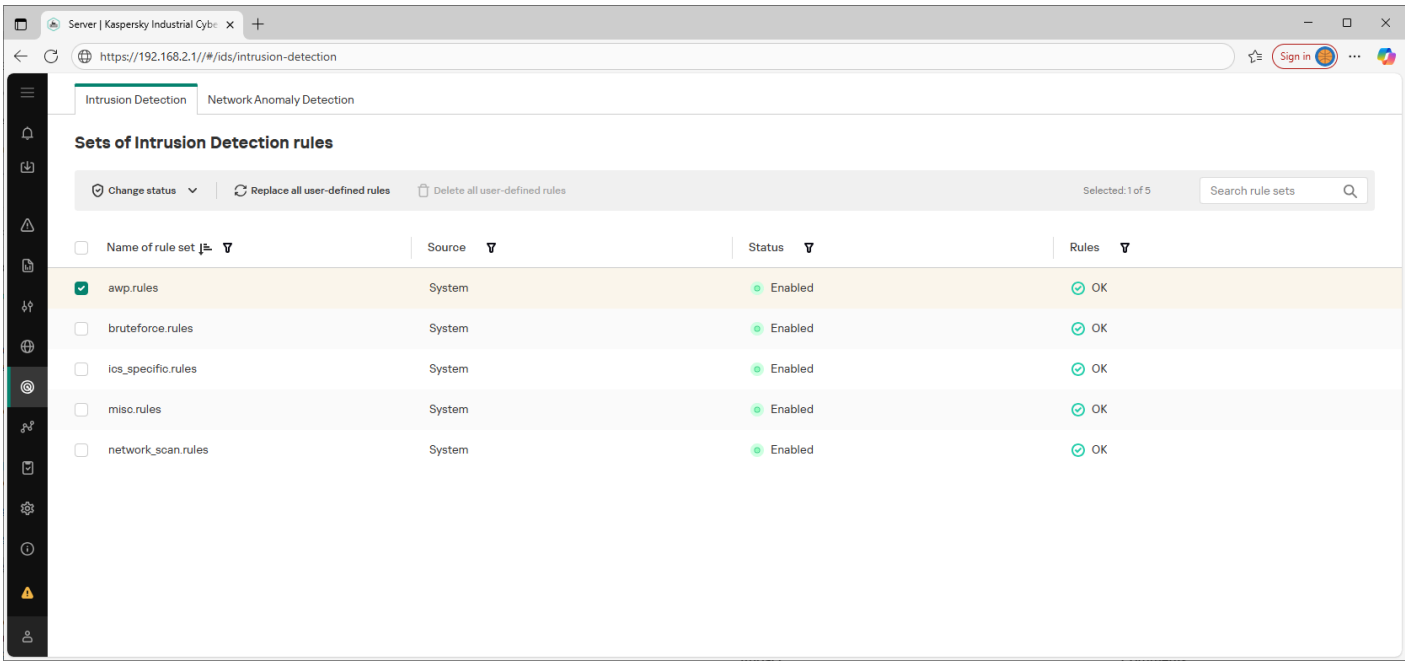
You can watch the tutorial video (see below) to familiarize yourself with the functionality.

https://www.youtube.com/watch?v=bluRipsZtO8

Industrial protocol Deep Packet Inspection

Detection rules section

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



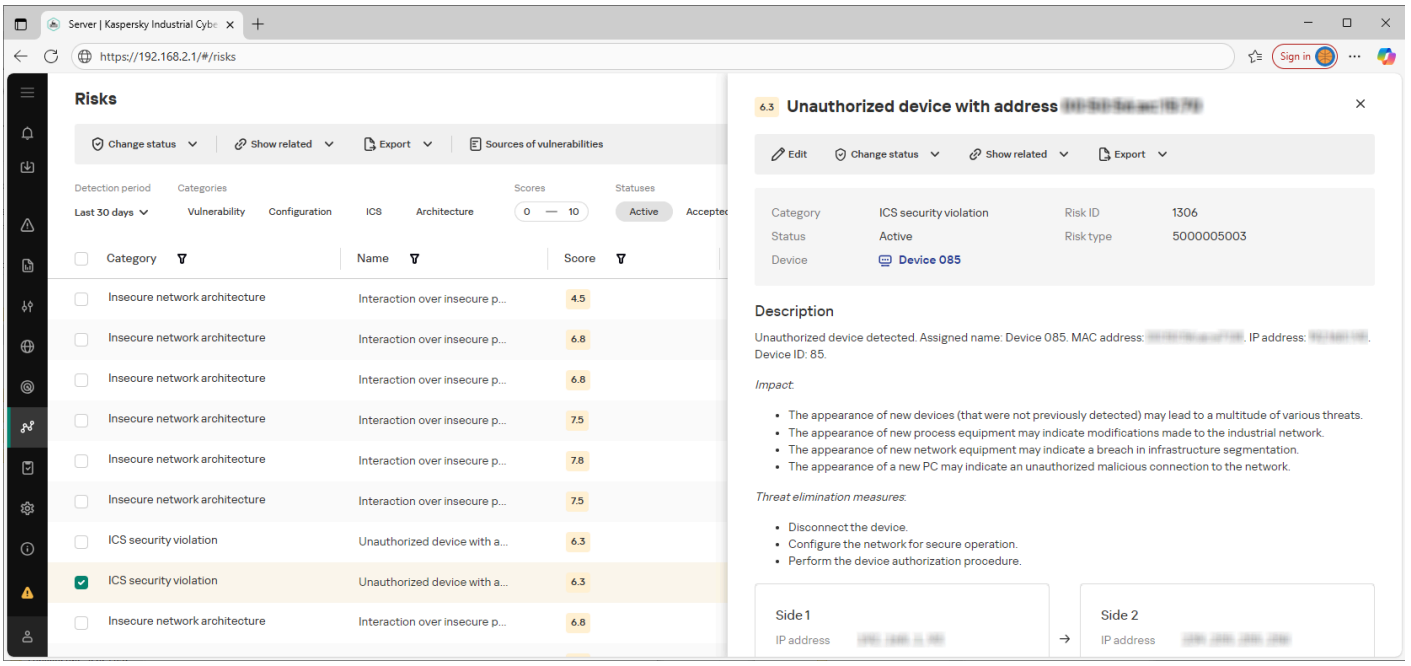
Detection rules section

The **Detection rules** section contains tabs with tables displaying sets of Intrusion Detection rules and Network Anomaly Detection rules.

When you select a rule in the Network Anomaly Detection rules table, the details area opens in the right part of the section. The details area contains information about the selected object and the tools for managing it.

Risks section

In the **Risks** section of the Application Server web interface (see the figure below), you can view and process risks detected by the application.



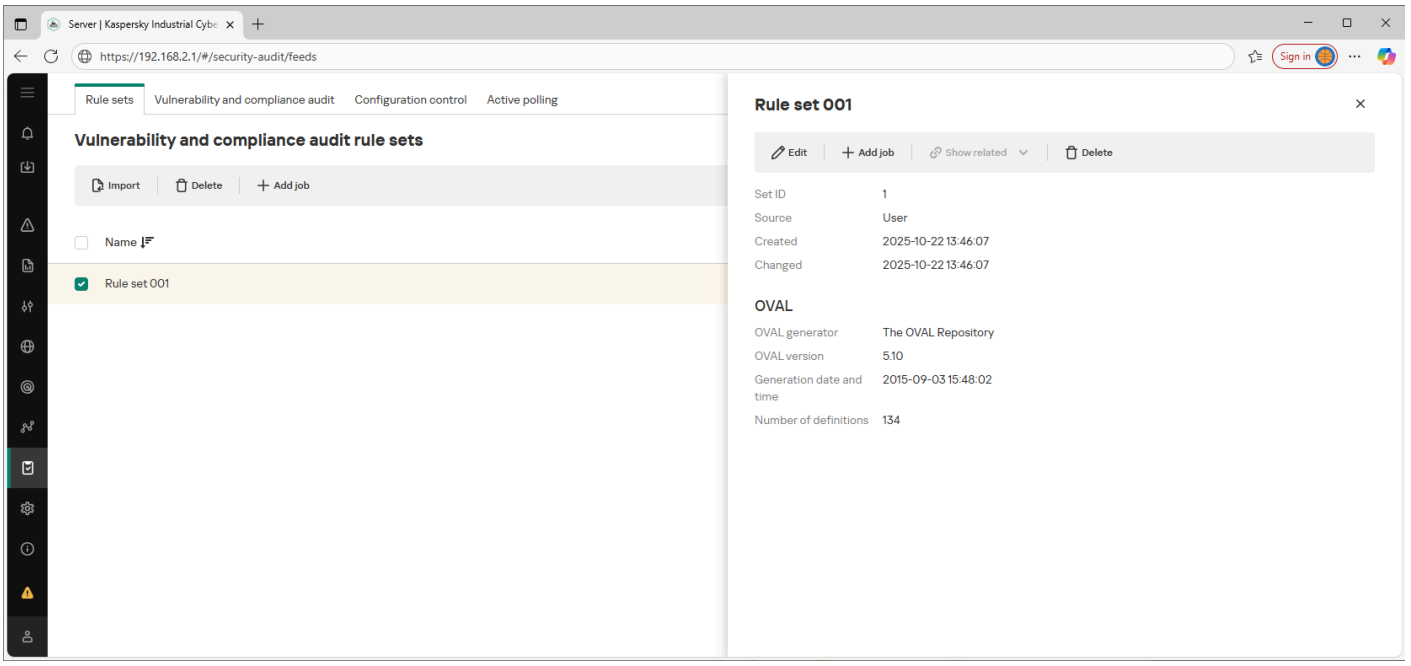
Risks section

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

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

Security audit section

In the **Security audit** section of the Application Server web interface (see the figure below), you can manage security audit jobs, as well as sets of rules for vulnerability and compliance audit jobs.



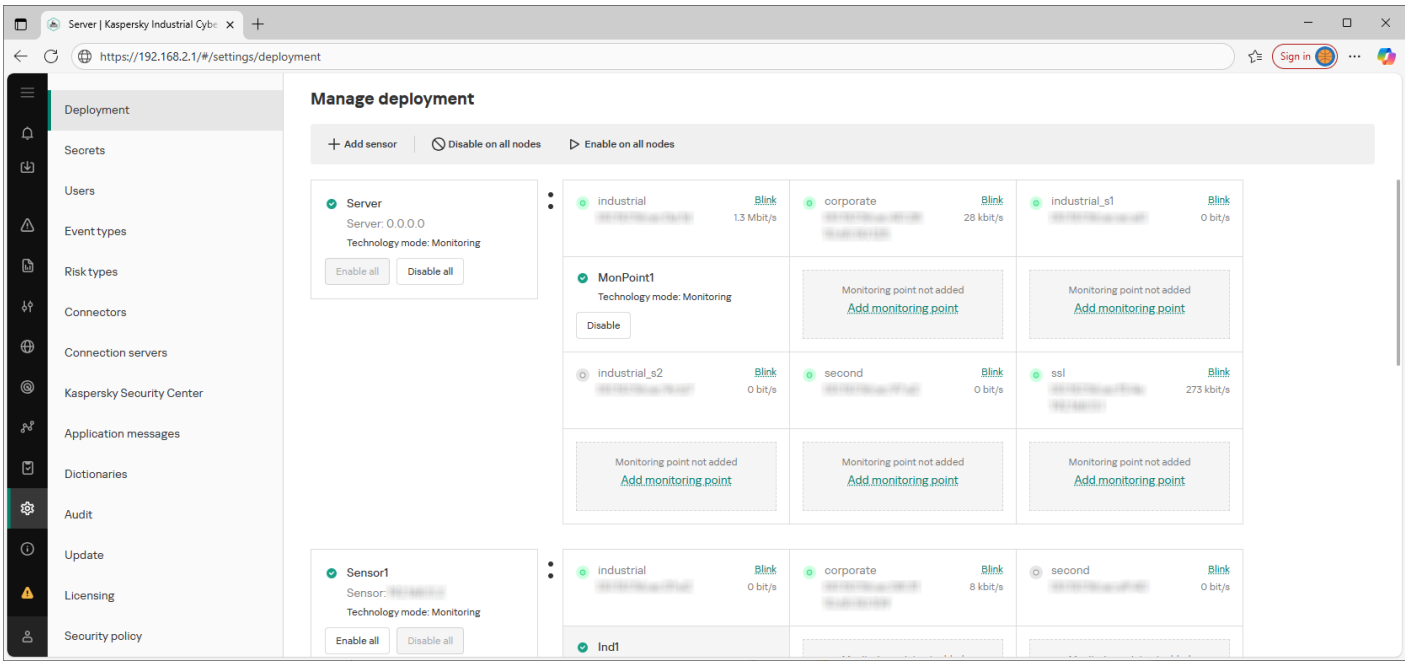
Security audit section

The **Security audit** section contains tabs with the tables of rule sets and jobs of various types.

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

Settings section

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



Settings section

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

- **Deployment**.

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

- **Secrets**.

  In this section, you can manage secrets containing account credentials for remote connections. The **Secrets** section is displayed if the connection to the Server is established using an account with any role except the Operator role.

- **Users**.

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

- **Event types**.

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

- **Risk types**.

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

- **Connectors**.

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

- **Connection servers**.

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

- **Kaspersky Security Center**.

  In this section, you can view and edit the settings for interaction with Kaspersky Security Center.

- **Application messages**.

  In this section, you can view application messages.

- **Dictionaries**.

  In this section, you can manage dictionaries for Network Anomaly Detection rules.

- **Audit**.

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

- **Update**.

  In this section, you can configure and run updates of application modules and databases. The **Update** section is displayed if an Administrator account was used to connect to the Server.

- **Licensing**.

  In this section, you can manage the license key for the application.

- **Security policy**.

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

- **Logging**.

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

Licensing the application

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

About the End User License Agreement

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

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

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

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

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

About the Privacy Policy

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

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

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

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

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

About the license

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

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

- Upd&Sup: for unlimited use of the basic functionality of the application, and for using the update functionality for application modules and databases during the license term.

  This type of license is used for licensing the Server and all employed application sensors. The update functionality is activated in the application after you add a license key with a valid license of the Upd&Sup type or a license key with a valid license of the Limited Updates type that was used for the previous versions of the application.

- Security Audit: for unlimited use of the basic functionality of the application, and for using the security audit functionality and the device active polling functionality during the license term.

  This type of license is used only for licensing the Application Server. To license the sensors that you will use, you must additionally purchase Upd&Sup licenses. The specified functionality is activated in the application after you add a license key with a valid license of the Security Audit type or a license key with a valid license of the Active Polling type that was used for the previous application versions.

- Remote Collector: for joint use with Kaspersky SD-WAN in the scenarios prescribed for integration mode.

  This type of license does not require you to add a license key to the application. However, if you have not purchased a Remote Collector license, you cannot use Kaspersky Industrial CyberSecurity for Networks in integration mode with Kaspersky SD-WAN.

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

When the license expires, the application continues to work but the corresponding functionality becomes unavailable. To continue using the corresponding functionality after the license has expired, you will need to add a new license key with a valid license of the required type.

Updates functionality (including providing anti-virus signature updates and codebase updates) may not be available in the software in the U.S. territory.

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 ID 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

License key (hereinafter also referred to as simply the *key*) is a sequence of bits that you can use to activate and then use the functionality that is determined by the license type. The license key is generated by Kaspersky experts.

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

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

About the license key file

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

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

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

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

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

You can add a license key to Kaspersky Industrial CyberSecurity for Networks in one of the following ways: when connected to the Server through the web interface or by using the functionality for automatic distribution of license keys to Kaspersky Security Center. This article describes the procedure for adding a license key when connected to the Server via the web interface.

When connected to the Server via the web interface, only users with the Administrator role can add a license key.

To add a license key:

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

   This opens the standard browser window for selecting a license key file.
4. Specify the path to the license key file with the KEY extension.
5. Click the button for opening the file.

The license key from the selected key file will be loaded into the application. After the key is loaded, the corresponding application functionality is activated. You can view information about the added license key.

Viewing information about an added license key

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

To view information about the license key:

Select **Settings** → **Licensing**.

The following information is displayed for an added license key:

- **Key** – unique alphanumeric sequence.
- **Description** – information about available functionality.
- **Activation date** – date when the license key was first added to the application.
- **Validity term** – license key expiration date.

- **Expires** – number of days remaining until expiration.
- Information about the key status or warning about a problem.

Removing a license key

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

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

To remove an added license key:

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

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

The license key will be removed from the application.

Data provision

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

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

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

- Names of user accounts that were created in the application (application users).
- IP addresses or names of computers with application components installed.
- IP addresses, MAC addresses, and other device information received by the application.
- Data on address spaces and subnets.
- Data on industrial process settings in Process Control rules.
- IP address or name of the computer hosting Kaspersky Security Center.
- IP addresses or names of computers that connect to the application through connectors.
- Email addresses of recipients indicated in email connectors and in report templates.
- Data in generated application reports.
- Data in industrial network traffic transmitted between devices and containing users' personal data (this data is processed by the application together with other data when analyzing industrial network traffic).
- Data on detected risks that could affect industrial system resources.
- Data on possibly infected objects or potential threats received from EPP applications and containing IP addresses, web addresses, and email addresses.
- Data on applications and patches received from EPP applications or as a result of security audit jobs.
- Data on executable files received from EPP applications or as a result of security audit jobs.
- Data on user accounts received from EPP applications or as a result of security audit jobs.
- Data on the results of checks performed on devices using the vulnerability and compliance audit rules.
- Data on device configurations received as a result of security audit jobs.
- Data on network sessions and protocol attributes.
- Identification and authentication information entered by the application user and saved in the secrets storage.

The listed data is processed to ensure the application operation in order to analyze violations of the technological process and to detect threats and anomalies in the network traffic that may be signs of attacks.

The application saves the received data in logs.

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

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

- Contents of folders used for storing application data:
  - Files of process logs for application components, the DBMS, and the Intrusion Detection system.
  - Files of working data of the Server and sensors.
  - Installation settings file created by the application centralized installation script.
  - Application message log and audit log.
- Security policy applied on the Server.
- Information about the current status of services supporting the operation of application components:
  - kics4net
  - kics4net-anomaly-hunter
  - kics4net-apm
  - kics4net-asset-config-repo
  - kics4net-asset-inventory
  - kics4net-blob-storage
  - kics4net-clickhouse
  - kics4net-config-control-orchestrator
  - kics4net-connectors
  - kics4net-connectors-launcher
  - kics4net-email-gateway
  - kics4net-epp-proxy
  - kics4net-fts
  - kics4net-nats-server
  - kics4net-oval-facade

- kics4net-postgresql
- kics4net-risk-oval-detector
- kics4net-report-builder
- kics4net-report-data-source
- kics4net-report-renderer
- kics4net-report-templates-catalog
- kics4net-report-templates-catalog-view
- kics4net-responses-manager
- kics4net-scan-oval-manager
- kics4net-scap-manager
- kics4net-scap-manager-view
- kics4net-scheduler
- kics4net-secrets
- kics4net-suricata
- kics4net-task-manager
- kics4net-task-manager-view
- kics4net-telemetry-proxy
- kics4net-vault
- kics4net-webserver
- kics4net-websensor
- klnagent

- Information about the version and distribution package of the operating system on computers that have application components installed (the `uname -a` command is used for receiving information).
- Information about the network interfaces on computers that have application components installed (the `ifconfig` command is used for receiving information).
- Entries saved by the auditd service in the file /var/log/audit/audit.log.
- Settings, status, and operating mode of the firewall in the operating system.

- If the corresponding settings are defined, the following files and data are also saved when running the application centralized installation script:
  - Traffic dump files.
  - Data on the Intrusion Detection system configuration.
  - Data on the certificates used in Kaspersky Industrial CyberSecurity for Networks (except certificates that were published by trusted certificate authorities).

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

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

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

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

Folders for storing application data

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

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

- Component and service installation folders:
  - /opt/kaspersky/kics4net/ – for the Server.
  - /opt/kaspersky/kics4net-anomaly-hunter/ – for the Rule-based Network Anomaly Detection service.
  - /opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /opt/kaspersky/kics4net-asset-config-repo/ – for the device configuration storage service.
  - /opt/kaspersky/kics4net-asset-inventory/ – for the service that processes the results of scanning device attributes using OVAL® rules.

- /opt/kaspersky/kics4net-blob-storage/ – for the service that stores arrays of binary data (Binary Large Object, BLOB).
- /opt/kaspersky/kics4net-cli/ – for the security policy export utility.
- /opt/kaspersky/kics4net-clickhouse/ – for a DBMS with a database for storing protocol attributes.
- /opt/kaspersky/kics4net-config-control-orchestrator/ – for the service that manages configuration control and active polling processes.
- /opt/kaspersky/kics4net-connectors/ – for system connectors.
- /opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
- /opt/kaspersky/kics4net-email-gateway/ – for the email notification forwarding service.
- /opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
- /opt/kaspersky/kics4net-fts/ – for the full-text search system.
- /opt/kaspersky/kics4net-nats-server/ – for the message broker.
- /opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
- /opt/kaspersky/kics4net-postgresql/ – for the DBMS with the Server database.
- /opt/kaspersky/kics4net-report-builder/ – for the report generation service.
- /opt/kaspersky/kics4net-report-data-source/ – for the service that provides data for reports.
- /opt/kaspersky/kics4net-report-renderer/ – for the service that provides visual representation of data blocks in reports.
- /opt/kaspersky/kics4net-report-templates-catalog/ – for the report template management service.
- /opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service that provides data on report templates.
- /opt/kaspersky/kics4net-task-manager/ – for the response task management service.
- /opt/kaspersky/kics4net-risk-oval-detector/ – for the service that processes the results of a device risk scan using OVAL rules.
- /opt/kaspersky/kics4net-scan-oval-manager/ – for the service that manages a device scan using OVAL rules.
- /opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.
- /opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
- /opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.
- /opt/kaspersky/kics4net-secrets/ – for the secrets repository interface service.

- /opt/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
- /opt/kaspersky/kics4net-task-manager/ – for the task management service.
- /opt/kaspersky/kics4net-task-manager-view/ – for the service that provides data on tasks.
- /opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /opt/kaspersky/kics4net-vault/ – for the service that stores secrets in the repository.
- /opt/kaspersky/kics4net-webserver/ – for the web server.
- /opt/kaspersky/klnagent64/ – for Network Agent, if installed.

- Folders for storing certificates and operational data:
  - /opt/kaspersky/kics4net/share/ids/ – for the Intrusion Detection system.
  - /var/opt/kaspersky/kics4net/ – for the Server.
  - /var/opt/kaspersky/kics4net-anomaly-hunter/ – for the Rule-based Network Anomaly Detection service.
  - /var/opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /va/opt/kaspersky/kics4net-asset-config-repo/ – for the device configuration storage service.
  - /var/opt/kaspersky/kics4net-asset-inventory/ – for the service that processes the results of a device risk scan using OVAL rules.
  - /var/opt/kaspersky/kics4net-blob-storage/ – for the BLOB service.
  - /var/opt/kaspersky/kics4net-cli/ – for the security policy export utility.
  - /var/opt/kaspersky/kics4net-clickhouse/ – for a DBMS with a database for storing protocol attributes.
  - /var/opt/kaspersky/kics4net-config-control-orchestrator/ – for the service that manages configuration control and active polling processes.
  - /var/opt/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
  - /var/opt/kaspersky/kics4net-email-gateway/ – for the email notification forwarding service.
  - /var/opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
  - /var/opt/kaspersky/kics4net-fts/ – for the full-text search system.
  - /var/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /var/opt/kaspersky/kics4net-oval-facade/ – for the service that scans remote devices using OVAL rules.
  - /var/opt/kaspersky/kics4net-postgresql/ – for the DBMS with the Server database.

- /var/opt/kaspersky/kics4net-report-builder/ – for the report generation service.
- /var/opt/kaspersky/kics4net-report-data-source/ – for the service that provides data for reports.
- /var/opt/kaspersky/kics4net-report-renderer/ – for the service that presents data blocks in reports.
- /var/opt/kaspersky/kics4net-report-templates-catalog/ – for the report template management service.
- /var/opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service that provides data on report templates.
- /var/opt/kaspersky/kics4net-responses-manager/ – for the response task management service.
- /var/opt/kaspersky/kics4net-risk-oval-detector/ – for the service that processes the results of a device risk scan using OVAL rules.
- /var/opt/kaspersky/kics4net-scan-oval-manager/ – for the service that manages a device scan using OVAL rules.
- /var/opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.
- /var/opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
- /var/opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.
- /var/opt/kaspersky/kics4net-secrets/ – for the secrets repository interface service.
- /var/opt/kaspersky/kics4net-task-manager/ – for the task management service.
- /var/opt/kaspersky/kics4net-task-manager-view/ – for the service that provides data on tasks.
- /var/opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /var/opt/kaspersky/kics4net-vault/ – for the service that stores secrets in the repository.
- /var/opt/kaspersky/kics4net-webserver/ – for the web server.
- /var/opt/kaspersky/klnagent/ – for Network Agent, if installed.

- Folders for storing process logs:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were centrally installed from this computer).
  - /var/log/kaspersky/kics4net/ – for the Server.
  - /var/log/kaspersky/kics4net-anomaly-hunter/ – for the Rule-based Network Anomaly Detection service.
  - /var/log/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/log/kaspersky/kics4net-asset-config-repo/ – for the device configuration storage service.
  - /var/log/kaspersky/kics4net-asset-inventory/ – for the service that processes the results of device attribute scans using OVAL rules.

- /var/log/kaspersky/kics4net-blob-storage/ – for the BLOB service.
- /var/log/kaspersky/kics4net-cli/ – for the security policy export utility.
- /var/log/kaspersky/kics4net-clickhouse/ – for a DBMS with a database for storing protocol attributes.
- /var/log/kaspersky/kics4net-config-control-orchestrator/ – for the service that manages configuration control and active polling processes.
- /var/log/kaspersky/kics4net-connectors/ – for system connectors.
- /var/log/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
- /var/log/kaspersky/kics4net-email-gateway/ – for the email notification forwarding service.
- /var/log/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
- /var/log/kaspersky/kics4net-fts/ – for the full-text search system.
- /var/log/kaspersky/kics4net-local-deploy/ – for storing the logs of local installation processes (if the Server was installed locally on this computer).
- /var/log/kaspersky/kics4net-nats-server/ – for the message broker.
- /var/log/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
- /var/log/kaspersky/kics4net-postgresql/ – for the DBMS with the Server database.
- /var/log/kaspersky/kics4net-report-builder/ – for the report generation service.
- /var/log/kaspersky/kics4net-report-data-source/ – for the service that provides data for reports.
- /var/log/kaspersky/kics4net-report-renderer/ – for the service that presents data blocks in reports.
- /var/log/kaspersky/kics4net-report-templates-catalog/ – for the report template management service.
- /var/log/kaspersky/kics4net-report-templates-catalog-view/ – for the service that provides data on report templates.
- /var/log/kaspersky/kics4net-responses-manager/ – for the response task management service.
- /var/log/kaspersky/kics4net-risk-oval-detector/ – for the service that processes the results of a device risk scan using OVAL rules.
- /var/log/kaspersky/kics4net-scan-oval-manager/ – for the service that manages a device scan using OVAL rules.
- /var/log/kaspersky/kics4net-scap-manager/ – for the security audit management service.
- /var/log/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
- /var/log/kaspersky/kics4net-scheduler/ – for the task scheduling service.
- /var/log/kaspersky/kics4net-secrets/ – for the secrets repository interface service.

- /var/log/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
- /var/log/kaspersky/kics4net-task-manager/ – for the task management service.
- /var/log/kaspersky/kics4net-task-manager-view/ – for the service that provides data on tasks.
- /var/log/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /var/log/kaspersky/kics4net-vault/ – for the service that stores secrets in the repository.
- /var/log/kaspersky/kics4net-webserver/ – for the web server (the web server also saves process data in the system log of the operating system).
- /var/log/kaspersky/klnagent64/ – for Network Agent, if installed.

- Folders for storing configuration files:
  - /etc/opt/kaspersky/kics4net/ – for the Server.
  - /etc/opt/kaspersky/kics4net-anomaly-hunter/ – for the Rule-based Network Anomaly Detection service.
  - /etc/opt/kaspersky/kics4net-asset-config-repo/ – for the device configuration storage service.
  - /etc/opt/kaspersky/kics4net-asset-inventory/ – for the service that processes the results of device attribute scans using OVAL rules.
  - /etc/opt/kaspersky/kics4net-blob-storage/ – for the BLOB service.
  - /etc/opt/kaspersky/kics4net-cli/ – for the security policy export utility.
  - /etc/opt/kaspersky/kics4net-clickhouse/ – for a DBMS with a database for storing protocol attributes.
  - /etc/opt/kaspersky/kics4net-config-control-orchestrator/ – for the service that manages configuration control and active polling processes.
  - /etc/opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
  - /etc/opt/kaspersky/kics4net-email-gateway/ – for the email notification forwarding service.
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
  - /etc/opt/kaspersky/kics4net-fts/ – for the full-text search system.
  - /etc/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /etc/opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /etc/opt/kaspersky/kics4net-report-builder/ – for the report generation service.
  - /etc/opt/kaspersky/kics4net-report-data-source/ – for the service that provides data for reports.
  - /etc/opt/kaspersky/kics4net-report-renderer/ – for the service that presents data blocks in reports.

- /etc/opt/kaspersky/kics4net-report-templates-catalog/ – for the report template management service.
- /etc/opt/kaspersky/kics4net-report-templates-catalog-view/ – for the service that provides data on report templates.
- /etc/opt/kaspersky/kics4net-responses-manager/ – for the response task management service.
- /etc/opt/kaspersky/kics4net-risk-oval-detector/ – for the service that processes the results of a device risk scan using OVAL rules.
- /etc/opt/kaspersky/kics4net-scan-oval-manager/ – for the service that manages a device scan using OVAL rules.
- /etc/opt/kaspersky/kics4net-scap-manager/ – for the security audit management service.
- /etc/opt/kaspersky/kics4net-scap-manager-view/ – for the service that provides data on security audit.
- /etc/opt/kaspersky/kics4net-scheduler/ – for the task scheduling service.
- /etc/opt/kaspersky/kics4net-secrets/ – for the secrets repository interface service.
- /etc/opt/kaspersky/kics4net-task-manager/ – for the task management service.
- /etc/opt/kaspersky/kics4net-task-manager-view/ – for the service that provides data on tasks.
- /etc/opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /etc/opt/kaspersky/kics4net-vault/ – for the service that stores secrets in the repository.
- /etc/opt/kaspersky/kics4net-webserver/ – for the web server.
- /etc/opt/kaspersky/klnagent/ – for Network Agent, if installed.
- /usr/lib/systemd/system/ – for storing configuration files for Kaspersky Industrial CyberSecurity for Networks services (for example, kics4net.service).
- /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file created during centralized installation of the application.
- /var/run/ – for storing variables of data on system health after loading in the folder itself (for example, the klnagent.pid file), or in subfolders (for example, the /kics4net/ subfolder).

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

- Component and service installation folders:
  - /opt/kaspersky/kics4net/ – for the sensor.
  - /opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /opt/kaspersky/kics4net-connectors/ – for system connectors.
  - /opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.

- /opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
- /opt/kaspersky/kics4net-nats-server/ – for the message broker.
- /opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
- /opt/kaspersky/kics4net-suricata/ – for the Intrusion Detection system.
- /opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /opt/kaspersky/kics4net-websensor/ – for the web server.
- /opt/kaspersky/klnagent64/ – for Network Agent, if installed.

- Folders for storing certificates and operational data:
  - /opt/kaspersky/kics4net/share/ids/ – for the Intrusion Detection system.
  - /var/opt/kaspersky/kics4net/ – for the sensor.
  - /var/opt/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/opt/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
  - /var/opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
  - /var/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /var/opt/kaspersky/kics4net-oval-facade/ – for the device scan service using OVAL rules without Network Agent.
  - /var/opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
  - /var/opt/kaspersky/kics4net-websensor/ – for the web server.
  - /var/opt/kaspersky/klnagent/ – for Network Agent, if installed.

- Folders for storing process logs:
  - /home/<user>/.config/kaspersky/kics4net-deploy/ – folder for storing installation process logs and the installation settings file (if application components were centrally installed from this computer).
  - /var/log/kaspersky/kics4net/ – for the sensor.
  - /var/log/kaspersky/kics4net-apm/ – for the active polling connector.
  - /var/log/kaspersky/kics4net-connectors/ – for system connectors.
  - /var/log/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.

- /var/log/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
- /var/log/kaspersky/kics4net-local-deploy/ – for storing the logs of local installation processes (if the sensor was installed locally on this computer).
- /var/log/kaspersky/kics4net-nats-server/ – for the message broker.
- /var/log/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
- /var/log/kaspersky/kics4net-suricata/ – for Intrusion Detection System.
- /var/log/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
- /var/log/kaspersky/kics4net-websensor/ – for the web server (the web server also saves process data in the system log of the operating system).
- /var/log/kaspersky/klnagent64/ – for Network Agent, if installed.

- Folders for storing configuration files:
  - /etc/opt/kaspersky/kics4net/ – for the sensor.
  - /etc/opt/kaspersky/kics4net-connectors-launcher/ – for the service that registers and starts manageable connectors.
  - /etc/opt/kaspersky/kics4net-epp-proxy/ – for the EPP application integration service in TCP mode.
  - /etc/opt/kaspersky/kics4net-nats-server/ – for the message broker.
  - /etc/opt/kaspersky/kics4net-oval-facade/ – for the service that performs remote device scanning using OVAL rules.
  - /etc/opt/kaspersky/kics4net-telemetry-proxy/ – for the EPP application integration service in UDP mode.
  - /etc/opt/kaspersky/kics4net-websensor/ – for the web server.
  - /etc/opt/kaspersky/klnagent/ – for Network Agent, if installed.
  - /usr/lib/systemd/system/ – for storing configuration files for Kaspersky Industrial CyberSecurity for Networks services (for example, kics4net.service).
  - /var/opt/kaspersky/kics4net-deploy/ – folder for storing a copy of the installation settings file created during centralized installation of the application.
  - /var/run/ – for storing variables of data on system health after loading in the folder itself or in subfolders.

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

About logs

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

Logs saved in the Server database

The application saves the following logs in the Server database:

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

For each log, you can set the size limit for storing records in the log storage settings.

The program monitors logging. If the occupied space of the audit log or message log of the program approaches the specified limit, the program displays a notification in the web interface menu. The notification is displayed in an open connection session of a user with the Administrator role.

To prevent the loss of important information in your logs due to automatic deletion of old entries, you can export the entries to a file. The program also allows you to configure automatic transfer of data from logs to third-party systems through connectors.

Logs saved in files

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

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

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

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

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

Administration of Kaspersky Industrial CyberSecurity for Networks

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

Deploying nodes

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

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

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

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

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

Adding and deleting sensors

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

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

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

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

Adding and connecting a sensor using the sensor web interface

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

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

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

Using a communication data package to add and connect a sensor

To add and connect a sensor using a communication data package:

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

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

3. Click **Add sensor**.

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

4. On the **Using a communication data package** tab:

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

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

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

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

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

The password must meet the following requirements:

- Must contain between 8 and 256 ASCII characters.
- Must contain one or more uppercase letters of the English alphabet.
- Must contain one or more lowercase letters of the Latin alphabet.
- Must contain one or more numerals.
- Must contain no more than three consecutive repeated characters.

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

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

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

Adding and connecting a sensor automatically over the network

To add and connect a sensor automatically over the network:

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

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

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

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

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

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

5. Click **Connect and add sensor**.

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

6. Connect to the sensor through the web interface.

   The sensor web interface page will show a message containing information about the certificate request fingerprint that was sent to the Server.

7. Make sure that the sequences of characters representing the certificate request fingerprint are identical on the web interface pages of the sensor and Server.

8. On the Server web interface page, click the button to confirm the received certificate request fingerprint.

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

Creating a new communication data package for a sensor

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

To create a new communication data package for a sensor:

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

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

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

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

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

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

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

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

      The password must meet the following requirements:

      - Must contain between 8 and 256 ASCII characters.
      - Must contain one or more uppercase letters of the English alphabet.
      - Must contain one or more lowercase letters of the Latin alphabet.
      - Must contain one or more numerals.
      - Must contain no more than three consecutive repeated characters.

6. Click **Create file**.

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

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

8. Connect to the sensor through the web interface.

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

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

Removing a sensor

Only users with the Administrator role can remove a sensor.

To remove a sensor:

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

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

3. Select the node tile of the sensor that you want to delete.

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

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Changing the main node settings

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

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

Changing the application data storage settings on a node

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

To change the maximum space limits:

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

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

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

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

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

Renaming a node that has application components installed

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

Only users with the Administrator role can change a node name.

To change the node name:

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

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

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

Connecting and configuring external storage for traffic dump files

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

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

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

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

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

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

   The details area will show the tabs for configuring the node parameters.
5. Select the **External storage** tab and use the **Connect external storage for traffic dump files** switch to enable external storage mode.
6. Specify the path in the local file system of the node to the directory intended for external storage.
7. Set the space limit for storing the traffic dump files under **Maximum size**.

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

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

Managing monitoring points on nodes

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

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

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

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

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

Adding a monitoring point

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

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

To add a monitoring point to a network interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Open the details area by clicking **Add monitoring point** in the tile of the relevant network interface. The link is displayed if a monitoring point has not been added to the network interface.

   The details area appears in the right part of the web interface window.
4. In the entry field in the upper part of the details area, enter the name of the monitoring point.

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

The monitoring point name must meet the following requirements:

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

5. Click **Add monitoring point**.

Enabling monitoring points

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

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

Only users with the Administrator role can enable monitoring points.

To enable monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Do one of the following:
   - If you want to enable one monitoring point, click **Enable** in the network interface tile containing the monitoring point. The button is available if the monitoring point is disabled.
   - If you want to enable all monitoring points on a node, click **Enable all** in the node tile hosting the disabled monitoring points. The button is available if the node has network interfaces with disabled monitoring points.
   - If you want to enable all monitoring points on all nodes, click **Enable on all nodes** in the toolbar.
4. Wait for the changes to be applied.

Disabling monitoring points

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

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

Only users with the Administrator role can disable monitoring points.

To disable monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Do one of the following:
   - If you want to disable one monitoring point, click **Disable** in the network interface tile containing the monitoring point. The button is available if the monitoring point is enabled.
   - If you want to disable all monitoring points on a node, click **Disable all** in the node tile hosting the enabled monitoring points. The button is available if the node has network interfaces with enabled monitoring points.
   - If you want to disable all monitoring points on all nodes, click **Disable on all nodes** in the toolbar.
4. Wait for the changes to be applied.

Renaming a monitoring point

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

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

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

To rename a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the network interface tile containing the monitoring point that you want to rename.

   The details area appears in the right part of the web interface window.
4. Click **Edit** and enter a new name in the field that appears.

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

   The monitoring point name must meet the following requirements:
   - Must be unique (not assigned to another monitoring point).
   - Must contain from 1 to 100 characters.
5. Click **Save**.

Deleting a monitoring point

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

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

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

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

To remove a monitoring point:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Deployment**.
3. Select the network interface tile containing the monitoring point that you want to delete.

   The details area appears in the right part of the web interface window.
4. In the details area, click **Delete**.

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

Identifying the Ethernet port associated with a network interface

A computer on which application components are installed may have multiple Ethernet ports used for connecting to the local area network. You can use the application to enable blink mode for a network interface and identify which Ethernet port is associated with this interface. When blink mode is enabled, the LED indicator next to the Ethernet port blinks for 15 seconds.

If the network interface does not support LED blink mode (for example, there is no LED indicator next to the Ethernet port or the network interface is a logical bonded interface), an error occurs when blink mode is enabled.

Only users with the Administrator role can enable Ethernet port blink mode.

To determine which Ethernet port is linked to a network interface:

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

3. Click **Blink** in the network interface tile.

   If the network interface supports an LED indicator, the network cable connection icon begins to blink on the network interface tile. At the same time, the LED indicator next to the Ethernet port begins to blink on the corresponding network adapter of the computer.

While blink mode is enabled for one network interface, you cannot enable blink mode for another network interface on the same node.

Managing technologies

Kaspersky Industrial CyberSecurity for Networks uses various technologies to analyze industrial network traffic. You can enable or disable the use of individual technologies. For some technologies, you can select the operation mode: learning mode or monitoring mode.

It is recommended to enable the technology learning mode for a predefined time so that the application automatically switches technologies to the monitoring mode at the right moment. The monitoring mode is a standard technology operation mode (as opposed to the learning mode, when the application only accumulates data for further use). When configuring the learning mode, you can set the desired time for the technology to automatically switch to the monitoring mode.

You can configure the same technology usage settings on all nodes and monitoring points or configure specific settings for the desired nodes and monitoring points. Technology usage settings can be automatically inherited from parent objects to child objects. If technology inheritance is enabled for a node or a monitoring point, the technology usage settings configured for the parent object (Server or sensor) are applied to this object. If technology inheritance is disabled, you can configure specific technology usage settings on this node or monitoring point.

After the application is installed, all technologies except for PLC Project Control and Unknown Tag Detection are enabled by default. The learning mode is enabled by default for the technologies supporting mode change. When adding sensors and monitoring points to the application, the inheritance of technologies set for the parent object is enabled for them by default.

Enabling and disabling technologies

You can enable or disable the use of technologies for the Server, sensors, and monitoring points. Enabling or disabling technologies on sensors and monitoring points is available if technology inheritance is disabled for these objects.

Some technologies include methods that can be enabled or disabled separately. If a technology or method is disabled, the application does not monitor communications of devices using this technology or method. You can configure the application settings related to the disabled technologies or methods (for example, add or edit rules).

The following technologies and methods can be enabled and disabled:

- Asset Management:
  - Device Activity Detection
  - Device Information Detection
  - PLC Project Control

- Network Session Detection
- Risk detection (only on the Server node)

- Network Control:
  - Network Integrity Control
  - Command Control
- Process Control:
  - Rule-based Process Control
  - Unknown Tag Detection
  - Device Discovery for Process Control
  - Get attributes of protocols
- Intrusion Detection:
  - Rule-based Intrusion Detection
  - ARP Spoofing Detection
  - IP Protocol Anomaly Detection
  - TCP Protocol Anomaly Detection
  - Brute-force Attack and Scan Detection

This article describes the procedure of enabling and disabling technologies on a Server node. The actions for enabling or disabling technologies on sensor nodes and monitoring points are performed in the same way after the technology inheritance is disabled for these objects.

Users with the Administrator or Security Officer role can enable and disable technologies on nodes.

To change the state of technologies and methods on the Server node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Settings** → **Deployment**.
3. Select the Server tile.

   The details area appears in the right part of the web interface window. The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled.

   If the states of technologies and methods cannot be currently changed, the switches in the list are disabled. In this case, it is recommended to check the status of the kics4net service on the Server computer. If the service is not active, you must start it.

4. Use the toggle switches on the left to enable or disable the use of relevant technologies and/or methods. You can enable or disable all technologies and methods simultaneously by clicking **Enable all** or **Disable all**.

5. After enabling or disabling a technology or method, wait for the changes to be applied. The toggle switch is unavailable until it is finished moving to the other state.

Configuring technology operating modes

You can configure the technology learning mode or manually enable the monitoring mode for the Server, sensors, and monitoring points. These actions are available on sensors and monitoring points if technology inheritance is disabled for these objects.

You can change the mode for the following technologies and methods:

- Device Activity Detection
- Command Control
- Rule-based Process Control
- Network Integrity Control

This section describes the procedure of changing and configuring technology modes on a Server node. The actions for changing and configuring technology modes on sensor nodes and monitoring points are performed in the same way after the technology inheritance is disabled.

Users with the Administrator or Security Officer role can change and configure the modes of technologies and methods on nodes.

To change and configure the modes of technologies and methods on the Server node:

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

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

3. Select the Server tile.

   The details area appears in the right part of the web interface window. The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled.

   > If the operation modes of technologies and methods cannot be currently changed, the switches in the list are disabled. In this case, it is recommended to check the status of the kics4net service on the Server computer. If the service is not active, you must start it.

4. For the technologies and methods supporting operation in the learning mode, in the drop-down list to the right of the technology or method name, select the relevant mode (**Learning** or **Monitoring**). If you want to select the same mode for all of these technologies and methods, use the **Mode** drop-down list.

   If different modes are selected, the **Mode** drop-down list displays the **Mixed** value.

5. After selecting the mode, wait for the changes to be applied. Before the mode is applied, the **Changing** status is displayed in the drop-down list.

6. For the technologies and methods operating in the learning mode, specify the date and time when they automatically switch to the monitoring mode. For this purpose, click **Set until** and select the date and time. If the date and time are configured before, they are displayed next to the mode name.

Managing inheritance of technologies

If you want a sensor or a monitoring point to automatically get the technology usage settings configured for a parent object, you can enable technology inheritance. In this case, the sensor gets the technology usage settings defined for the Server, and the monitoring point gets the settings defined for the node for which the monitoring point is added (for the Server or a sensor).

If necessary, you can disable technology inheritance on a sensor or monitoring point. This allows you to configure specific technology usage settings for this object.

Users with the Administrator or Security Officer role can enable and disable technology inheritance on a sensor or monitoring point.

To enable or disable technology inheritance on a sensor node:

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

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

3. Select the sensor tile.

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

4. Set the **Inherit Server technologies** switch to the desired position.

To enable or disable technology inheritance on a monitoring point:

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

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

3. Select the network interface tile with the monitoring point for which you want to enable or disable technology inheritance.

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

4. Set the technology inheritance switch to the desired position.

Downloading traffic received by the node monitoring points

You can download traffic received by the application through monitoring points on nodes. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads traffic from the traffic dump file storages. Both the internal storage of each node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.

To download traffic received by the node monitoring points:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Deployment**.
3. Do one of the following:
   - To download traffic received by the monitoring points of a certain node, select the tile of this node.
   - To download traffic received by a specific monitoring point, select the network interface card with this monitoring point.

   The details area appears in the right part of the web interface window.
4. Click **Download traffic**. If the button is not displayed in the toolbar, click the ⋮ button and select the desired item in the menu that opens.
5. Do the following in the opened window:
   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

     The default period is one hour.
   - Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

     If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.
   - When a node tile is selected, if necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points of the node that receives the traffic (this section is displayed if a node tile is selected).

     By default, all monitoring points available on the selected node are specified.
   - If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets belong (this section is displayed if additional address spaces are added to the application).

     By default, all address spaces created in the application are specified.
   - If necessary, enable filtering in the **Filtering using BPF** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

     Filtering expression example

     ```
     tcp port 102 or tcp port 502
     ```

- If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets.

  ```
  Filtering expression example
  ```

  ```
  ^test.+xABxCD
  ```

6. Click **Download**.
7. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the button in the menu of the application web interface.

   The list of background operations appears.

   b. Wait for the file generation operation to complete.

   c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Monitoring the state of Kaspersky Industrial CyberSecurity for Networks

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

Monitoring the application state when connected through the web interface

You can view information about the current state of the application when connected to the Server through the web interface. The application state is monitored by using the relevant widgets in the **Dashboard** section.

The application also informs about disabled protection functions and operational issues.

Information about disabled protection functions

If certain protection functions are disabled, the **Not all protection services are running** notification is displayed in the lower part of the menu on the application web interface page. The notification is displayed in the following cases:

- One or more monitoring points are disabled.
- One or more protection functions are disabled (for example, rule-based Intrusion Detection).
- Learning mode is enabled for one or more protection functions (for example, Network Integrity Control technology).

To view information about disabled protection functions:

1. Click the **Not all protection services are running** notification.

   The **Components not providing protection** window opens.

2. Select one of the following tabs:

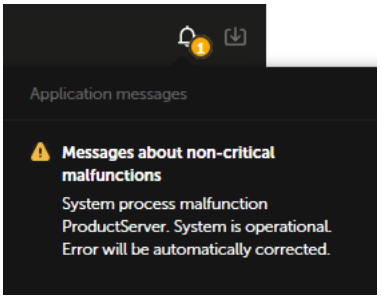
   - **Server** – to view the details of disabled Server protection services.

     If technology inheritance is enabled on the nodes of the sensors and monitoring points, the **Inheritance of technologies on all components is enabled** message is displayed in the upper right corner of the **Server** tab.

   - **Sensors** – to view the details of disabled sensor protection services.
   - **Monitoring points** – to view the details of disabled monitoring points protection services.

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).



List of notifications about problems in application operation in the browser window

If the list contains notifications about critical problems (for example, messages about disruption of application operation), a red icon is displayed. If the list contains only notifications about non-critical problems, a yellow icon is displayed.

The list contains only up-to-date notifications. If a problem has been resolved (for example, a lost connection with the Server has been restored), the corresponding notification is automatically removed from the list.

You can view detailed information about notifications (except notifications regarding unavailability of the Server or database).

To view information about a notification:

1. In the menu, click the button.
2. In the list of notifications, click the text of the notification.

   The browser window will show the section containing information pertaining to the notification (for example, under **Settings** → **Application messages**).

Viewing application messages

The application message log stores information about errors in application operation and about errors in operations performed by system processes of Kaspersky Industrial CyberSecurity for Networks.

You can view application messages when connected to the Server through the web interface. If necessary, you can also configure forwarding of application messages to recipient systems via connectors.

To view application messages:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Application messages**.

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

The settings of application messages are displayed in the following columns of the table:

- **Date and time**

  Date and time when the application message was registered.

- **Status**

  Status of the message. The following statuses are available for messages:

  - *Normal operation* – for informational messages.
  - *Unknown*, *Malfunction* – for messages about non-critical application errors.
  - *Moderate malfunction, Critical malfunction*, *Fatal malfunction* – for messages about application malfunctions.

- **Node**

  Name or IP address of the node from which the message originated.

- **System process**

  Application process that invoked message registration.

- **Message**

  Numerical identifier and text of the message.

When viewing the application messages table, you can use the filter, search, and sorting functions and export data.

Viewing user activity audit entries

Kaspersky Industrial CyberSecurity for Networks can save information about actions performed by users in the application. Information is saved in the audit log if user activity audit is enabled.

You can view audit entries when connected to the Server through the web interface. If necessary, you can also configure the forwarding of audit entries to recipient systems via connectors.

Only users with the Administrator role can view audit entries.

To view audit entries:

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

2. Select **Settings** → **Audit**.

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

The settings of audit entries are displayed in the following columns of the table:

- **Date and time**

  Date and time when the user action data was registered.

- **Action**

  Action attempted by the user.

- **Result**

  Result of the registered action (successful or unsuccessful).

- **User**

  Name of the user who performed the action.

- **User role**.

  Role of the user who performed the action.

- **User node**

  IP address of the node on which the action was attempted.

- **Description**

  Registered action code and description of the result.

When viewing the audit entries table, you can use the configuration, filter, search, and sorting functions and export data.

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

Users with any role can view information about nodes with application components installed and about network interfaces on nodes.

To view information about nodes and network interfaces:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Deployment**.

   The web interface window displays node tiles (on the left) and network interface tiles detected on these nodes (on the right of each node).
3. If you want to view detailed information about a node or network interface, select the tile of the relevant node or network interface.

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

Displayed information about nodes with application components installed

A node tile displays the following information:

- Current node status.
  - *OK* The node is available, and no application messages about non-critical malfunctions or disrupted operation were received from this node.
  - *Non-critical malfunction*. The node is available, and application messages with a status of *Unknown* or *Malfunction* were received from this node.
  - *Operation disrupted*. The node is available, and application messages with a status of *Moderate malfunction*, *Critical malfunction* or *Fatal malfunction* were received from this node.
  - *No connection*. The node is unavailable.
- Node name.
- Application component installed on the node: **Server** or **Sensor**.
- IP address for connecting to the node (address 0.0.0.0 corresponds to all possible IP addresses on the computer).
- The current mode of the technologies for which the operating mode can be selected. The tile contains the mode name (*Learning* or *Monitoring*) if all technologies are running in that mode. If different modes are selected for the technologies, the *Mixed* value is displayed.
- If the inheritance of Server technologies is disabled for a sensor, the icon is displayed.

Displayed information about network interfaces

A network interface tile displays the following information:

- Icon showing if a network cable is connected to the Ethernet port of the network interface:
  - – the network cable is connected.
  - – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.
- Network interface name in the operating system.
- MAC address.
- Rate of incoming traffic received by the network interface.
- Information about the monitoring point (if one was added):
  - Current status of the monitoring point:
    - *OK*. The monitoring point is available.
    - *Switchover*. The operating mode of the monitoring point is being changed.
    - *Error*. An error was detected when switching over the operating mode of the monitoring point.
  - Monitoring point name.
  - Current operating mode of the monitoring point:
    - If the monitoring point is disabled, the *Disabled* value is displayed.
    - If the monitoring point is enabled, the current mode of the technologies for which the operating mode can be selected is displayed. The tile contains the mode name (*Learning* or *Monitoring*) if all technologies are running in that mode. If different modes are selected for the technologies, the *Mixed* value is displayed.
  - If the inheritance of the node technologies is disabled for a monitoring point, the icon is displayed.

Node information displayed in the details

The details area displays the following information for the selected node:

- Node name.
- The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled on the node.

  For the technologies with a selectable operating mode, the current mode is displayed: **Learning** or **Monitoring**. If learning mode is enabled, the date and time of the automatic switching to the monitoring mode are displayed to the right of the mode name (the date and time are not displayed if the time of the automatic switching is not set).
- The **Settings** tab displays the following information:
  - **Status** – current node status indicated by an icon and text description (same as on the node tile).
  - **Node type** – application component installed on the node: **Server** or **Sensor**.
  - **Disk space currently used by the application** – disk space occupied by application files. This includes the installed files and files that are created while the application is running.
  - **Maximum disk space that can be used by the application** – disk space that can be occupied by application files. This includes the installed files and the sum of all volume limits defined in data storage rules. This value cannot exceed the available disk space.
  - **Occupied on disk** – disk space used by all files. This includes application files and files of the operating system and other applications. This volume of space is calculated on the drive that contains the /var/ folder in the file system of the node.
  - **Free disk space** – disk space that is not used by files. This volume of space is calculated on the drive that contains the /var/ folder in the file system of the node.
  - **Total disk space** – total volume of disk space on the drive that contains the /var/ folder in the file system of the node.
  - **Inheritance of technologies** – flag that indicates whether the inheritance of Server technologies is enabled or disabled (only for sensor nodes).
  - **BPF filtering** flag that indicates that the node has enabled or disabled filtering using the Berkley Packet Filter (BPF) technology based on address parameters in network packets.
  - **Retention rules** – current and maximum values of the following settings: volume, number of items and storage time of the application data.

Network interface information displayed in the details

For a network interface to which a monitoring point is not added, the following information is displayed in the details area:

- **Network interface** – name of the network interface in the operating system.
- **Connection** – icon indicating that a network cable is connected to the Ethernet port of the network interface:
  - – the network cable is connected.
  - – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.
- **MAC address** – MAC address of the network interface.
- **IP address** – IP address of the network interface. If multiple IP addresses are detected on a network interface, the details area displays no more than 16 IP addresses.

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

- Monitoring point name.
- **Status** – current status of the monitoring point indicated by an icon and text description:
  - *OK*. The monitoring point is available.
  - *Switchover*. The operating mode of the monitoring point is being changed.
  - *Error*. An error was detected when switching over the operating mode of the monitoring point.
- **Connection** – icon indicating that a network cable is connected to the Ethernet port of the network interface:
  - – the network cable is connected.
  - – the network cable is disconnected.

  The icon blinks when Ethernet port blink mode is enabled.
- **Network interface** – name of the network interface in the operating system.
- **Mode** – current operating mode of the monitoring point:
  - *Enabled*.
  - *Disabled*.

- The **Manage technologies** tab displays the list of technologies and methods that can be enabled or disabled on the monitoring point.

  For the technologies with a selectable operating mode, the current mode is displayed: *Learning* or *Monitoring*. If learning mode is enabled, the date and time of the automatic switching to the monitoring mode are displayed to the right of the mode name (the date and time are not displayed if the time of the automatic switching is not set).

- On the **Settings** tab:

  - **Inheritance of technologies** – flag that indicates whether the inheritance of the node technologies is enabled or disabled.

  - **MAC address** – MAC address of the network interface.

  - **IP address** – IP address of the network interface. If multiple IP addresses are detected on a network interface, the details area displays no more than 16 IP addresses.

Viewing the status of services supporting operation of application components

You can view the status of services supporting the operation of application components. If the service is active, this means that it was successfully started.

To view the status of a service:

1. On the computer on which the application component is installed, open the operating system console.

2. Enter the following command:

   ```
   sudo service <service name> status
   ```

   where `<service name>` is the name of the service, whose information you want to view. You can specify the following services:

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

   - `kics4net-anomaly-hunter` – service for rule-based detection of network anomalies (runs on a computer that performs Server functions).

   - `kics4net-apm` – active polling connector service (runs on a computer that performs Server or sensor functions).

   - `kics4net-asset-config-repo` – device configuration storage service (runs on the computer that performs the Server functions).

   - `kics4net-asset-inventory` – service for processing the results of scanning device attributes using OVAL rules (runs only on a computer that performs Server functions).

   - `kics4net-blob-storage` – service for storing arrays of binary data (runs only on a computer that performs Server functions).

- `kics4net-clickhouse` – DBMS service with a database for storing protocol attributes (runs only on a computer that performs Server functions).
- `kics4net-config-control-orchestrator` – service for managing configuration control and active polling processes (runs only on the computer that performs the Server functions).
- `kics4net-connectors-launcher` – registration and launch of manageable connectors service (runs on a computer that performs Server functions or sensor functions)
- `kics4net-email-gateway` – service for sending email notifications (runs only on a computer that performs Server functions).
- `kics4net-epp-proxy` – service for integration with EPP applications in TCP mode (runs on a computer that performs Server or sensor functions).
- `kics4net-fts` – full-text search system service (runs only on a computer that performs Server functions).
- `kics4net-nats-server` – message broker service (runs on a computer that performs Server functions or sensor functions).
- `kics4net-oval-facade` – service for scanning remote devices using OVAL rules (runs on a computer that performs Server or sensor functions).
- `kics4net-postgresql` – DBMS service (runs only on a computer that performs Server functions)
- `kics4net-report-builder` – service for generating reports (runs only on a computer that performs Server functions).
- `kics4net-report-data-source` – service for providing data for reports (runs only on the computer that performs Server functions)
- `kics4net-report-renderer` –service for visual display of data blocks in the reports (runs only on the computer that performs Server functions)
- `kics4net-report-templates-catalog` – service for managing report templates (runs only on the computer that performs Server functions)
- `kics4net-report-templates-catalog-view` – service for providing data about the report templates (runs only on the computer that performs Server functions)
- `kics4net-responses-manager` – service for managing the response jobs (runs only on the computer that performs Server functions)
- `kics4net-risk-oval-detector` – service for processing the results of device risk scans using OVAL rules (runs only on the computer that performs Server functions)
- `kics4net-scan-oval-manager` – service for managing device scanning using OVAL rules (runs only on the computer that performs Server functions)
- `kics4net-scap-manager` – service for managing security audit (runs only on the computer that performs Server functions)
- `kics4net-scap-manager-view` – service for providing security audit data (runs only on the computer that performs Server functions)

- `kics4net-scheduler` – task scheduling service (runs only on a computer that performs Server functions).
- `kics4net-secrets` – service for the secrets repository facade (runs only on the computer that performs Server functions)
- `kics4net-task-manager` – task management service (runs only on a computer that performs Server functions)
- `kics4net-task-manager-view` – service for providing data about tasks (runs only on the computer that performs Server functions)
- `kics4net-telemetry-proxy` – service for integration with EPP applications in UDP mode (runs on a computer that performs Server or sensor functions).
- `kics4net-vault` – service for storing secrets in the repository (runs only on the computer that performs Server functions)
- `kics4net-websensor` – web server service (runs only on a computer that performs sensor functions).
- `kics4net-webserver` – web server service (runs only on a computer that performs Server functions).
- `klnagent` –Network Agent service (runs only on a computer that performs Server functions).

Example

```
sudo service kics4net status
```

If the service is not active, you can restart the computer or restart the service.

Restarting a computer that has application components installed

When restarting a computer that performs Server or sensor functions, application components are automatically started. A restart does not affect the subsequent operation of these components (except in some situations when there is a malfunction after an unexpected restart).

A restart may be required in the following cases:

- There is not enough free space on the computer hard drive.
- The computer was unexpectedly restarted, after which the operation of application components was not restored.
- One of the application services is not active.
- A lost connection between the Server and a sensor is not being restored. In this case, you should restart the computer that performs sensor functions.

You can use the standard commands of the operating system to restart a computer that has application components installed.

If the computer cannot be restarted for some reason, you can restart the services supporting operation of application components.

To restart services:

1. Open the operating system console.
2. Depending on which functions are performed by the computer, do the following:

   - If the computer performs Server functions, enter the following sequence of commands:

```
sudo service kics4net-postgresql restart
sudo service kics4net-config-control-orchestrator restart
sudo service kics4net-asset-inventory restart
sudo service kics4net-blob-storage restart
sudo service kics4net-email-gateway restart
sudo service kics4net-fts restart
sudo service kics4net-report-builder restart
sudo service kics4net-report-data-source restart
sudo service kics4net-report-renderer restart
sudo service kics4net-report-templates-catalog restart
sudo service kics4net-report-templates-catalog-view restart
sudo service kics4net-responses-manager restart
sudo service kics4net-risk-oval-detector restart
sudo service kics4net-scap-manager restart
sudo service kics4net-scap-manager-view restart
sudo service kics4net-scan-oval-manager restart
sudo service kics4net-scheduler restart
sudo service kics4net-secrets restart
sudo service kics4net-task-manager restart
sudo service kics4net-task-manager-view restart
sudo service kics4net-vault restart
sudo service kics4net-webserver restart
sudo service kics4net-asset-config-repo restart
sudo service kics4net-anomaly-hunter restart
sudo service kics4net-clickhouse restart
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-telemetry-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
sudo service klnagent restart
```

   - If the computer performs sensor functions, enter the following sequence of commands:

```
sudo service kics4net restart
sudo service kics4net-connectors-launcher restart
sudo service kics4net-epp-proxy restart
sudo service kics4net-telemetry-proxy restart
sudo service kics4net-nats-server restart
sudo service kics4net-oval-facade restart
sudo service kics4net-websensor restart
```

Using a test network packet to verify event registration

To verify the registration of events in Kaspersky Industrial CyberSecurity for Networks, you can use a test network packet. When this type of packet is detected in traffic, the application registers test events based on the following technologies:

- Deep Packet Inspection An event is registered regardless of whether or not there are Process Control rules or tags.
- Network Integrity Control An event is registered regardless of whether or not there are Interaction Control rules. Use of Network Integrity Control technology must be enabled.

- Intrusion Detection An event is registered regardless of whether or not there are Intrusion Detection rules. Use of Rule-based Intrusion Detection must be enabled.
- Asset Management An event is registered regardless of whether or not there are known devices in the table of devices. Use of device activity detection must be enabled.

Events are registered with system event types that are assigned the following codes:

- 4000000001 for an event based on Deep Packet Inspection technology.
- 4000000002 for an event based on Network Integrity Control technology.
- 4000000003 for an event based on Intrusion Detection technology.
- 4000000004 for an event based on Asset Management technology.

You can view test events in the table of registered events.

To verify audit functions, Kaspersky Industrial CyberSecurity for Networks saves information about the registration of test events in the audit log. An audit entry is created for each registered event, and this entry specifies the technology used to register the test event.

A test network packet is a UDP protocol packet with certain parameter values. The parameters are defined in such a way as to exclude the probability of receiving such a packet in normal industrial network traffic.

The following data must be defined in the parameters of a test network packet:

- Ethernet II header:
  - Source MAC address: `00:00:00:00:00:00`
  - Destination MAC address: `ff:ff:ff:ff:ff:ff`
  - EtherType: `0x0800 (IPv4)`
- IP header:
  - Source IP address: `127.0.20.20`
  - Destination IP address: `127.0.20.20`
  - ID: `20`
  - TTL: `20`
  - Protocol type: `17 (UDP)`
  - Flags: `0x00`
- UDP header:
  - Source port: `20`
  - Destination port: `20`

- Packet contents:
  - Length of packet contents, in bytes: `20`
  - Packet contents: "`KICS4Net Sentinel 20`"

To generate and send a test network packet, you can use a network packet generator program such as Scapy. You need to send the test network packet from a node whose traffic is controlled by Kaspersky Industrial CyberSecurity for Networks.

To send a test network packet using the program Scapy in a Linux® operating system:

1. In the operating system console of the computer, enter the command to run Scapy in interactive mode:

   ```
   sudo scapy
   ```

2. Enter the command to send the test network packet:

   ```
   sendp(
    Ether(src='00:00:00:00:00:00', dst='ff:ff:ff:ff:ff:ff')/
    IP(src='127.0.20.20', dst='127.0.20.20', id=20, ttl=20)/
    UDP(sport=20, dport=20)/
    "KICS4Net Sentinel 20",
    iface="<interface name>"
   )
   ```

   where `<interface name>` is the name of the network interface connected to the industrial network (for example: `eth0`).

After the packet is detected in traffic, Kaspersky Industrial CyberSecurity for Networks registers test events.

Checking the integrity of application modules

You can check the integrity of installed software modules to make sure that there were no changes to those modules after installation. This check is performed by comparing the checksums of installed application modules with their reference values. An integrity check must be run separately on each node hosting installed application modules.

You can run an integrity check on a node in the following ways:

- Run the check locally using the kics4net-manifest-checker-<application version>.bundle.sh script.
- Run when connecting to the Server through the web interface.

Running an integrity check locally using a script

The kics4net-manifest-checker-<application version>.bundle.sh script is included in the Kaspersky Industrial CyberSecurity for Networks distribution kit. The script checks the application module files against special lists that are stored in the *manifest files*. The manifest files are included in the application installation packages and contain file lists of the corresponding packages. Each application package has a corresponding manifest file. The manifest files are digitally signed and their integrity is also verified.

If you make any changes to the kics4net-manifest-checker-<application version number>.bundle.sh script file, its results may be invalid. For valid results, use only that version of the script which is include in the Kaspersky Industrial CyberSecurity for Networks distribution kit.

While running, the script sequentially checks the checksums of files from the application packages installed in the operating system.

To check the integrity of application modules on a node computer by using the kics4net-manifest-checker-<application version>.bundle.sh script:

1. Copy to any folder the script file kics4net-manifest-checker-<application version number>.bundle.sh from the folder with unpacked script files and packages for installing, validating and removing application components, contained in the distribution kit. The files are located in the kics4net-release_<application version>/linux-centos subfolder.

2. In the operating system console, go to the folder containing the script file, and enter the following command:

   ```
   sudo bash kics4net-manifest-checker-<application version number>.bundle.sh
   ```

   Information about the results of the check are displayed in the operating system console.

The results of the software module integrity check on the computer are considered successful if the following two conditions are met:

- The kics4net-manifest-checker-<application version number>.bundle.sh script terminates with the message: `All files of installed packages containing the manifest file have been successfully checked`.
- All application packages that should be installed on the computer in accordance with their proper functions do not return error messages or at least do not return either of the following messages:
  - `The package is not installed in the operating system`.
  - `The manifest file for the package could not be found`.

Running an integrity check when connected to the Server through the web interface

You can run an integrity check of application modules on a node when connected to the Server through the web interface. An integrity check started in this way is performed using similar methods as the kics4net-manifest-checker-<application version>.bundle.sh script.

To check the integrity of application modules on a node computer when connected to the Server through the web interface:

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

   The details area appears in the right part of the web interface window.
4. Click **Check integrity**. If the button is not displayed in the toolbar, click the ⋮ button and select the desired item in the menu that opens.

   You will see a message informing you that an integrity check was started, and information about its progress will be available in the list of background operations for some time. If necessary, you can view the current list of background operations by clicking the button in the application web interface menu.
5. To view the integrity check results, go to **Settings** → **Application messages**.

The results of an integrity check of application modules on a computer are deemed successful if the list of application messages includes the following message for the corresponding node: `Integrity check of application modules on node completed successfully`.

If the list of application messages does not include a message indicating a successful integrity check but instead contains an error message, the integrity check is deemed unsuccessful. You can identify the application packages that did not pass the integrity check by using the kics4net-manifest-checker-<application version>.bundle.sh script (see above).

Synchronizing the time on nodes of Kaspersky Industrial CyberSecurity for Networks with the time source used for industrial network devices

To correctly correlate the time of registration of events with the time when events occurred in the industrial network, time must be synchronized in the system. The time on nodes with Kaspersky Industrial CyberSecurity for Networks components installed must be synchronized with a common source of time used by industrial network devices.

When centrally installing Kaspersky Industrial CyberSecurity for Networks, you can enable automatic time synchronization between the Server and nodes where sensors are installed. In this case, the node with the Server installed will serve as the time source for nodes that have sensors installed. It is recommended to use the software tools from the operating system of the computer performing Server functions to configure time synchronization between the Server and the common time source used by devices in the industrial network. For Server time synchronization, you can use the standard protocols known as Network Time Protocol (NTP) and Precision Time Protocol (PTP).

NTP is used for automatic time synchronization between the Server and other nodes. In this case, you cannot configure synchronization with other time sources or use the PTP protocol on nodes that have sensors installed.

If a sensor was installed locally using the kics4net-install.sh script, automatic time synchronization with the Server is not performed on this node. If this is the case, you must configure time synchronization on the Server and on all nodes containing sensors that were installed locally.

For example sequences of operations for configuring time synchronization, please refer to the Appendices.

Updating databases and application modules

Kaspersky Industrial CyberSecurity for Networks provides the capability to update the following databases and application modules:

- System Intrusion Detection rules.
- Network Anomaly Detection rule templates.
- Modules for processing application-layer protocols for industrial process control purposes.
- Event correlation rules for registering incidents.
- Rules for obtaining information about devices and communication protocols.
- Industrial equipment vulnerabilities database.
- Kaspersky Digital Signature (KDS) certificate revocation list.
- Application functionality configuration.

- System sets of rules for vulnerability and compliance audit jobs.
- OpenSSL cryptographic module.
- Kaspersky ICS CERT vulnerabilities database for SCADA.
- Methods for identifying techniques of potential attacks based on system command detection events.

Application modules and databases are updated after installing updates released by Kaspersky.

Timely installation of updates ensures maximum protection of an industrial network using Kaspersky Industrial CyberSecurity for Networks. In addition, these updates can augment and update application modules involved in providing security for the application. Failure to regularly install updates over time will increase the risks to application security due to the emergence of new threats. You must also install security updates for your particular operating system.

It is recommended to manually start installing updates immediately after you install components of Kaspersky Industrial CyberSecurity for Networks. You can configure automatic scheduled start settings for regular installation of updates.

You can use the following update sources:

- Kaspersky update servers.
- Kaspersky Security Center Administration Server.

For an update source, you can also use files from a local resource if installation of updates is started manually.

You can configure the settings and start the installation of updates when connected to the Server through the web interface.

Updates of databases and application modules are subject to the following limitations and special considerations:

- Update functionality is available after a license key is added. A license key with a valid Security Audit license provides the capability to update all application modules and databases. If a key with an Upd&Sup license is added, the application does not activate the functionality for updating system sets of rules for vulnerability and compliance audit jobs.

  Updates functionality (including providing anti-virus signature updates and codebase updates) may not be available in the software in the U.S. territory.

- After installing the OpenSSL library update, restart the services on the nodes with the installed application components.
- To download updates from Kaspersky update servers, you must have Internet access. When connected to update servers from a computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server, the connection is established over the HTTPS protocol (connection through a proxy server is not supported).
- To download updates from the Kaspersky Security Center Administration Server to Kaspersky Industrial CyberSecurity for Networks, the capability for application interaction with Kaspersky Security Center must be added. You can add this functionality during installation or reinstallation of Kaspersky Industrial CyberSecurity for Networks. Updates are downloaded from the Administration Server repository, which obtains its updates through the corresponding task in Kaspersky Security Center.

Manually starting an update

You can run an update at any time. The capability to run an update is available after a license key is added.

Only users with the Administrator role can manually start an update.

To manually start an update:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.
3. Under **Source for manual update**, select one of the following options for update sources:
   - Local update source – lets you download updates from files via a specific local path. You can click **Browse** to specify the local path to files.
   - **Kaspersky update servers** – for downloading updates from Kaspersky update servers.
   - **Kaspersky Security Center Administration Server** – for downloading updates from the Kaspersky Security Center Administration Server. This option is available if the capability for application interaction with Kaspersky Security Center has been added.
4. Click **Update now**.

Configuring automatic updates

After adding a license key, you can configure automatic updates by schedule.

Only users with the Administrator role can configure automatic updates by schedule.

To enable and configure automatic updates by schedule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.
3. Use the **Start scheduled update** toggle to enable automatic updates.
4. Under **Source for scheduled update**, select one of the following options for update sources:
   - **Kaspersky update servers** – for downloading updates from Kaspersky update servers.
   - **Kaspersky Security Center Administration Server** – for downloading updates from the Kaspersky Security Center Administration Server. This option is available if the capability for application interaction with Kaspersky Security Center has been added.

5. Define the update schedule settings. To do so:

    a. In the **Frequency** drop-down list, define when the updates have to occur. Select one of the following options: **Hourly**, **Daily**, **Weekly**, or **Monthly**.

    b. Depending on the selected option, specify the values for the settings defining the precise update run schedule.

6. Click **Save settings**.

Viewing information about update installation

You can view general and detailed information about update installation.

General information about installed updates

General information provides the dates and times when the updated application modules and databases were released.

To view general information about installed updates:

On the application web interface page, select the **About** section.

Detailed information about update installation

Detailed information contains information about update installation processes that are started. The application saves the following detailed information:

- Date and time when the update process was started
- Update run mode
- Date and time of release of the databases and application modules installed during the update process (if the update was successful)
- Error information (if the update failed)
- List of updated databases and application modules

Detailed information about update installation is saved in the application message log.

Restarting services on the nodes after installing the OpenSSL library update

If the OpenSSL library update is installed on the nodes where the application components are installed, restart the services that ensure the operation of application components on these nodes. The services on the sensor nodes are restarted automatically. If restart of the services on the Server node is required, the application displays notifications about it on the Server web interface page. In this case, to restart the services, you can restart the Server computer or initiate a restart on the web interface page.

Notifications about the need to restart the services on the Server node are displayed in the list of notifications about problems in the application operation, as well as under **Settings** → **Update**.

Only the users with the Administrator role can initiate a restart of the Server services on the web interface page.

To restart the services on the Server node using the Server web interface:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Update**.
3. In the **Restart required** notification, click **Restart Server**.

   The service restart process starts. The Application Server is not available for connections until the restart process is complete. During the service restart process, the application web interface page displays a special section named **Application maintenance**.

Distributing access to application functions

In Kaspersky Industrial CyberSecurity for Networks, you can restrict users' access to application functions depending on the tasks of specific users.

The following user accounts may be used to access the application:

- User accounts created in the application.
- Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

It is not possible to connect to the Server under other user accounts or using anonymous connections.

User accounts that have access to the application do not have to be registered as operating system user accounts on the Server computer.

The first application user account must be created during startup configuration of Kaspersky Industrial CyberSecurity for Networks. Then you can create additional user accounts that will be used to perform actions in the application.

Depending on which component you are connected to through the web interface, the following sets of functions are available:

- Application functions when connected to the Server
- Application functions when connected to a sensor

When connected to the Server, the application provides access to functions depending on the role of the user that established the connection.

About application user accounts

Role-based access control (RBAC) is used to restrict access to application functions. The role of an application user account determines the set of actions available to the user. The following roles are provided for application user accounts:

- **Administrator**.

  A user with this role has all the access rights necessary to administer the application, manage its operation, perform monitoring, and view information. This user can also access functions for managing user accounts created in the application.

- **Security officer**.

  It is recommended to assign this role to employees who are responsible for the security of the industrial facility. A user with this role has the access rights necessary to monitor the system and manage registered events and incidents. This user has the capability to initiate response actions in the application.

- **Infrastructure expert**.

  It is recommended to assign this role to employees who are responsible for the infrastructure of the industrial facility (network equipment, workstations, and others). A user with this role has the access rights necessary to receive information about devices and their interactions and to configure allow rules.

- **ICS expert**.

  It is recommended to assign this role to employees who are responsible for the operation of the control system at the industrial facility. A user with this role has the access rights necessary to monitor industrial network assets and device-related risks. To update the employee's available information about devices, SCADA and PLC projects, this user has the capability to configure and run security audit jobs.

- **Operator**.

  It is recommended to assign this role to employees who are security system operators. A user with this role has the minimum set of access rights necessary for monitoring and viewing information. This user also has the capability to assign Active statuses to events and incidents based on their processing results.

The Administrator role is assigned to the first user account that is created during startup configuration of the application.

When adding subsequent user accounts, you can assign the appropriate roles to them. You can create up to 100 user accounts for users of the application (not counting users that are configured for Single Sign-On from Kaspersky Security Center).

When connected to the Server, users receive the access privileges corresponding to the role of their user account. If the role of an application user is changed by another user (who has been assigned the Administrator role) while the user is working, the access rights of the connected user are updated in online mode. For example, a user that has connected to the Server with the Administrator role will lose the rights to access application management functions after the Operator role is assigned to their user account.

Only users with the Administrator role can manage user accounts and view their information. Information about user accounts created in the application is displayed under **Settings** → **Users** in the Kaspersky Industrial CyberSecurity for Networks web interface.

Application functions that are available when connected to the Server through the web interface

This article presents the application functions that are available to users when connected to the Server through the web interface (see the table below).

Available application functions depending on the user role

Application function	Administrator	Security Officer	Infrastructure Officer	ICS Officer	Operator
Monitoring the application state when connected through the web interface	✓	✓	✓	✓	✓
Viewing application messages	✓	✓	✓	✓	✓
Enabling and disabling the user activity audit	✓				
Viewing user activity audit entries	✓				
Viewing information about nodes with application components installed and about network interfaces on nodes	✓	✓	✓	✓	✓
Running an application module integrity check when connected to the Server through the web interface	✓	✓			
Adding and deleting sensors	✓				
Changing the main node settings	✓				
Managing monitoring points on nodes	✓				
Managing technologies	✓	✓			
Downloading traffic received by the node monitoring points	✓	✓	✓	✓	✓
Viewing information about an added license key	✓	✓	✓	✓	✓
Adding a license key	✓				
Removing a license key	✓				
Configuring automatic updates	✓				
Manually starting an update	✓				
Viewing information about update installation	✓	✓	✓	✓	✓
Viewing information about application user accounts	✓				
Creating an application user account	✓				
Changing the role of an application user account	✓				
Administrator-initiated password change	✓				
Managing user lockout	✓				
Deleting an application user account	✓				

Application function	Administrator	Security Officer	Infrastructure Officer	ICS Officer	Operator
Changing your account password	✓	✓	✓	✓	✓
Functions when viewing data tables	✓	✓	✓	✓	✓
Viewing device information	✓	✓	✓	✓	✓
Selecting sources for device vulnerability monitoring	✓	✓			
Configuring address spaces	✓	✓	✓		
Manually adding devices	✓	✓	✓	✓	
Merging devices	✓	✓	✓	✓	
Deleting devices	✓	✓	✓	✓	
Changing the statuses of devices	✓	✓	✓	✓	
Creating a device group tree	✓	✓	✓	✓	
Automatic grouping of devices based on a specific criterion	✓	✓	✓	✓	
Manually arranging devices into groups	✓	✓	✓	✓	
Adding and removing labels for devices	✓	✓	✓	✓	
Editing device information	✓	✓	✓	✓	
Adding, editing and deleting custom fields for a device	✓	✓	✓	✓	
Deleting device users	✓	✓			
Removing device executable files	✓	✓			
Assigning a golden device configuration	✓	✓	✓	✓	
Comparison of saved device configurations	✓	✓	✓	✓	✓
Resetting deviations in the network behavior of devices	✓	✓	✓	✓	✓
Viewing address space rules	✓	✓	✓	✓	✓
Viewing address space subnets	✓	✓	✓	✓	✓
Viewing information about devices with IP addresses from the selected subnets	✓	✓	✓	✓	✓
Managing Process Control settings for devices	✓	✓	✓	✓	
Managing tags	✓	✓		✓	
Managing Process Control rules	✓	✓		✓	
Monitoring process parameter values	✓	✓	✓	✓	✓
Viewing Interaction Control rules in the table of allow rules	✓	✓	✓	✓	✓
Fine-tuning Interaction Control for individual devices	✓	✓	✓	✓	
Manually creating Interaction Control rules	✓	✓	✓	✓	
Editing Interaction Control rule settings	✓	✓	✓	✓	
Enabling and disabling Interaction Control rules	✓	✓	✓	✓	
Suspending and resuming monitoring of the network interactions of devices	✓	✓	✓	✓	
Deleting Interaction Control rules	✓	✓	✓	✓	
Enabling and disabling sets of Intrusion Detection rules	✓	✓			
Loading and replacing user-defined sets of Intrusion Detection rules	✓	✓			
Removing user-defined sets of Intrusion Detection rules	✓	✓			
Managing Network Anomaly Detection rules	✓	✓			
Managing dictionaries for Network Anomaly Detection rules	✓	✓			

Application function	Administrator	Security Officer	Infrastructure Officer	ICS Officer	Operator
Managing the settings for storing log entries in the database	✓				
Managing the settings for saving traffic in the database	✓				
Managing the settings for saving traffic dump files	✓				
Managing the settings for storing report files	✓				
Changing the logging level for processes	✓				
Configuring operation with EPP applications	✓				
Managing response actions	✓	✓			
Enabling and configuring interaction with Kaspersky Security Center	✓				
Managing connectors	✓				
Adding and deleting connector types	✓				
Managing vulnerability and compliance audit jobs	✓	✓	✓	✓	
Receiving reports on vulnerability and compliance audit jobs	✓	✓	✓	✓	✓
Viewing general information about the vulnerability and compliance audit job runs	✓	✓	✓	✓	✓
Managing storage settings for the runs of vulnerability and compliance audit jobs	✓				
Managing sets of rules for vulnerability and compliance audit jobs	✓	✓			
Managing configuration control jobs	✓	✓	✓	✓	
Viewing general information about the configuration control job runs	✓	✓	✓	✓	✓
Managing active device polling jobs	✓	✓	✓	✓	
Viewing general information about the active polling job runs	✓	✓	✓	✓	✓
Managing account credentials secrets for remote connections	✓	✓	✓	✓	
Configuring event types	✓				
Changing the base score for a risk type	✓				
Managing the settings for storing risks	✓				
Exporting a security policy to a file	✓	✓	✓	✓	✓
Importing a security policy from a file	✓				
Clearing the current security policy	✓				
Live system monitoring	✓	✓	✓	✓	✓
Working with the network interaction map	✓	✓	✓	✓	✓
Moving nodes and groups to other groups on the network interaction map	✓	✓	✓	✓	
Downloading traffic when working with the network interaction map	✓	✓	✓	✓	✓
Viewing network session details	✓	✓	✓	✓	✓
Downloading network session traffic	✓	✓	✓	✓	✓
Forming a topology map	✓	✓	✓	✓	
Viewing details about objects on the topology map	✓	✓	✓	✓	✓
Monitoring events and incidents	✓	✓	✓	✓	✓
Managing reports and report templates	✓	✓			
Manually generating reports	✓	✓	✓	✓	✓
Exporting reports to a file	✓	✓	✓	✓	✓

Application function	Administrator	Security Officer	Infrastructure Officer	ICS Officer	Operator
Viewing risk details	✓	✓	✓	✓	✓
Manually changing the statuses of risks	✓	✓	✓	✓	

Viewing information about application user accounts

When connected to the Server through the web interface, you can view information about user accounts that were created in the application. The application does not display information about Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

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

To view information about application user accounts:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.

   The table displays users that match the filter and search criteria.

The following columns display user settings:

- **Name**

  Specified user name

- **Role**.

  Specified user role

- **Status**

  Current status of user. The following statuses are available:

  - **Allowed**: the account has not been locked by an Administrator, or the account is unlocked.
  - **Blocked**: the account has been locked by an Administrator.

    The application assigns the **Blocked** status to the account only as a result of actions performed by the administrator. A temporary restriction on connecting to the Server via the web interface for an account does not result in the assignment of the **Blocked** status.

  - **Suspicious activity**: the user entered the wrong password for their account several times in a row.

- **Created**

  Date and time when the user was added to the application.

- **Changed**

  Date and time when the user settings were last modified.

When viewing the user table, you can use configuration, filtering, search, and sorting.

Creating an application user account

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

To create an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Open the details by clicking **Add user**.
4. In the user name entry field, enter a user name for the account you want to create.

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

   The user account name must meet the following requirements:

   - Must be unique within the list of application user names (not case-sensitive).
   - Must contain 3-20 characters.
   - Must begin with a letter.
   - Must end with any supported character except a dot.
5. In the drop-down list, select the necessary user role.
6. In the password entry fields, enter the password that you want to set for the user account.

   The password must meet the following requirements:

   - Must contain between 8 and 256 ASCII characters.
   - Must contain one or more uppercase letters of the English alphabet.
   - Must contain one or more lowercase letters of the Latin alphabet.
   - Must contain one or more numerals.
   - Must contain no more than three consecutive repeated characters.
7. If you want the user to change the password the first time they connect to the application, select the **Require password change at next logon** check box.
8. Click **Save**.

A new user account will appear in the user table.

Changing the role of an application user account

When connected to the Server through the web interface, you can change the roles of user accounts that were created in the application. This role modification method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

Only users with the Administrator role can change the roles of user accounts.

Users with the Administrator role can change the role of any user account except the role of their own user account.

To change the role of an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Select the user whose role you want to change.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. In the drop-down list, select the necessary user account role.
6. Click **Save**.

Administrator-initiated password change

An Administrator can set a new password for any other user. To change their own password, an Administrator, like any other user, must follow the password change procedure.

An Administrator can set a new password for an account created in the application only. This password change method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

We recommend changing user passwords in the following cases:

- The user account is unlocked.
- The password has been compromised.
- The **Suspicious activity** status has been assigned to the account, or notifications about unsuccessful user logon attempts are displayed at the top of the web interface menu.

To set a new password for an account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.

3. Select the user you want to set a new password for.

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

4. Click **Set new password**. If the button is not displayed in the toolbar, click the ⋮ button and select the desired item in the menu that opens.

   A **Changing user password** window appears.

5. Enter the new password in the **New password** and **Repeat new password** fields.

   The new password must meet the requirements listed in **Changing user password**. The conditions you fulfill are automatically marked while you are entering your password.

6. If you want the user to change the password the next time they connect to the application, select the **Require password change at next logon** check box.

7. Enter your password in the **Confirmation password** field.

8. Click **Save**.

The user will need the new password next time they connect via the web interface.

Managing user lockout

An Administrator can lock any other user's account. Once the reasons for the Administrator-initiated lockout have been addressed, an Administrator can unlock the account.

When an account is locked, the application resets the password expiration date and terminates the user's current session. Once the account is unlocked, the password expiration date remains reset. Therefore, after unlocking, the user needs to set a new password.

After unlocking a user account, we recommend immediately setting a new password to prevent malicious actors from guessing the old password and hijacking the unlocked account. An Administrator can either set a new password or supervise the password change at the user's computer.

An Administrator can lock or unlock accounts created in the application only. These actions are not available to Kaspersky Security Center user accounts configured for Single Sign-On (SSO).

To lock a user account:

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

2. Select **Settings** → **Users**.

3. Select the user you want to lock.

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

4. Click **Block**.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

To unlock a user previously locked by an Administrator:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Select the user you want to unlock.

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

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

Deleting an application user account

When connected to the Server through the web interface, you can delete user accounts that were created in the application. This deletion method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

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

A user with the Administrator role can delete any user account except their own user account.

To delete an application user account:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Users**.
3. Select the user you want to delete.

   The details area appears in the right part of the web interface window.
4. Click **Delete**. If the button is not displayed in the toolbar, click the ⋮ button and select the desired item in the menu that opens.

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

Configuring Asset Management

Kaspersky Industrial CyberSecurity for Networks lets you monitor the assets of a company as represented by its industrial network devices. Devices are identified by the application based on their MAC- and/or IP addresses. The application can receive device data when doing the following:

- Processing traffic arriving through monitoring points
- Processing data received from EPP applications

A table of devices is created for the purpose of asset management in the application. The table is populated based on the address spaces configured in the application.

The application can automatically obtain information about devices. Only information that can be identified by the application may be automatically obtained and updated (for example, address information of a device).

For device activity detection and automatic update of information, the corresponding Asset Management methods must be enabled. If necessary, you can manually specify the values of specific data and disable their automatic update to lock the current values (for example, you can lock the device category if the currently defined category differs from the one that is determined automatically).

Some device information must be specified manually because it cannot be automatically updated. For example, you can save specific device information in the table of devices, and add any absent criteria for sorting and filtering devices. You can also use manually defined information to arrange devices in various groups in the group tree, or filter and search for devices based on device labels.

You can configure Asset Management and edit device information in the **Assets** section of the **Devices** tab. You can also view information about the interactions between devices and perform various actions with devices when working with the network interaction map and with the topology map. To conveniently present information about interactions between devices and to enable automatic grouping of devices by subnet, you can generate lists of subnets in the address space based on the specific IP addressing of devices in your company's network.

Asset Management methods and modes

The following methods are used for asset management in Kaspersky Industrial CyberSecurity for Networks:

- Device Activity Detection This method lets you monitor the activity of devices in industrial network traffic based on the obtained MAC- and/or IP addresses of devices.
- Device Information Detection This method lets you automatically get and update information about devices known to the application, using data received from traffic or other sources as the basis.
- PLC Project Control. This method lets you detect information about PLC projects in traffic, save this information in the application, and compare it to previously obtained information.
- Risk Detection. This method lets you detect information security risks based on information about devices and their interactions.
- Network Session Detection. This method analyzes industrial network traffic to detect network sessions created by devices for the purpose of connecting to other devices.

You can enable and disable the use of individual asset management methods.

About the device activity detection method

The following modes are available for the device activity detection method:

- Learning mode. This mode is intended for temporary use. In this mode, all devices whose activity is detected in traffic are considered to be authorized by the application. You can enable learning mode only for the device activity detection method. The device activity detection method can be applied together with other asset management methods.

- Monitoring mode. This mode is intended for continual use. In this mode, when activity of devices is detected, the application considers only those devices that have been assigned the *Authorized* status as authorized.

Depending on the selected mode, the application automatically assigns statuses to devices.

In learning mode, the application does not register events when it detects activity of devices or when device information is automatically updated.

You can configure the learning mode for the device activity detection method. Asset management learning mode must be enabled for a sufficient amount of time to detect the activity of relevant devices. This amount of time depends on the number of devices in the industrial network and how frequently they operate and are serviced. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period from one to several days to detect the activity of all required devices.

The received MAC- and IP addresses of devices are processed with the following special considerations:

- A router indicator must be set for devices that perform functions of a network switch between industrial network segments. If this indicator is not defined automatically by the application, it must be set manually. Otherwise, the application may fail to populate the table of devices with devices that interact through this routing device in different industrial network segments. After the indicator is set, interacting devices will be added to the table of devices when there is corresponding traffic involving them.

- If only the device IP address is detected in traffic (the IP address cannot be matched to a specific MAC address), this IP address is checked against the list of subnets known to the application. The device activity detection method ignores IP addresses that belong to **Public** subnets only.

About the device information detection method

When the device information detection method is enabled, the application automatically updates information about known devices. For example, the application can update the name of the operating system installed on a device as it detects updated data in the traffic of the device.

By default, automatic update is enabled for all information. For some types of information, in the device settings, you can disable automatic update in the following cases: adding a device manually, merging devices, and changing the device information.

To automatically get information about devices, the application can use:

- Built-in *rules for detection of information about devices and device communication protocols*.

  After installation, the application uses the default rules for identifying information about devices and the protocols of communication between devices. To increase the accuracy of identifying information, Kaspersky experts regularly update the databases containing the sets of rules. You can update rules by installing updates.

- Data from EPP applications containing information about the devices.

  The application processes data from EPP applications, which contain information about devices (for example, equipment information).

- Data from EPP applications processed according to the rules from the *Kaspersky ICS CERT vulnerabilities database for SCADA*.

  Rules from the Kaspersky ICS CERT vulnerabilities database for SCADA provide for additional analysis of data received from EPP applications. Based on the analysis results, the application can indirectly determine some information about the devices (for example, the device category). The **Kaspersky ICS CERT vulnerabilities database for SCADA** is a system-based set of security audit rules. These rule set is supplied and updated together with the database and application module updates. Therefore, to use the rules from this set, install the updates.

About events registered when applying methods

In monitoring mode, the application registers the corresponding events based on Asset Management technology. Depending on the applied methods, events may be registered in the following cases:

- Detection of activity of unknown devices or devices that have a status of *Archived*.
- Automatic change of device information.
- Detection of read/write operations with projects and PLC project blocks.
- Detection of Vulnerability risks and changes related to these risks.

When PLC Project Control is enabled, the application may register a large number of events associated with the detection of read/write operations with projects or blocks. Normally, a large number of events are registered at the initial stage when this method is used. To reduce the total number of registered events, the PLC Project Control method is disabled by default after the application is installed. You can enable this method at any time.

Selecting sources of vulnerability data

When monitoring risks, the application detects vulnerabilities of devices by using information from the database of known vulnerabilities. Kaspersky experts upload vulnerability information to the database from various data sources.

By default, the application detects vulnerabilities of devices based on the information that has been uploaded to the database from all sources. If necessary, you can select relevant sources to detect vulnerabilities of devices based on the information from only these sources.

Only users with the Administrator or Security Officer role can select sources for device vulnerability detection.

To enable or disable use of sources for vulnerability detection:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. In the **Risks** section, click **Sources of vulnerabilities** to open the window for selecting sources.
3. Enable or disable the use of specific sources. The list contains all sources in the database of known vulnerabilities.
4. Click **Apply**.

Manually adding devices

This section provides instructions on manually adding devices. You can manually add a new device to the table of devices. For an added device, you must specify its MAC address and/or IP address.

> The MAC- and IP addresses of an added device must be unique within the address space containing these addresses. If additional address spaces were added to the application, you can add devices with identical addresses to different address spaces.

Users with any role except the Operator role can add devices manually.

After adding a device, you can add Process Control settings for the device.

Adding a device when working with the table of devices

To add a device to the table of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.
2. On the **Devices** tab in the **Assets** section, open the details area by clicking **Add device**.
3. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.
4. On the **Address information** tab in the details area, specify the MAC and/or IP addresses of the device.
5. If additional address spaces were added to the application, specify the names of the address spaces for addresses.

6. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:

   - If you want to add an IP address, click **Add IP address**.
   - If you want to remove an IP address, click the icon located on the right of the field containing the IP address.

7. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To do so, perform one of the following actions:

   - If you want to add a network interface, click **Add interface** under the group of settings of the last network interface of the device.
   - If you want to delete a network interface, click the icon displayed to the right of the device network interface name (if there are two or more network interfaces).
   - If you want to define a different name for a network interface, click the icon located on the right of the current name and enter the new name for the network interface in the field that opens.

8. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the and icons. On the **Settings** tab, the and icons are located on the left side of the fields. On the **Address information** tab, the and icons are located to the right of the network interface name.

9. On the **Custom fields** tab in the details area, create a list of custom fields if needed.

10. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the icon.

The table of devices will show the new device with a status of *Authorized*.

Adding a device when working with the topology map

When working with the topology map, you can add a new device to the table of devices.

To add a new device to the table of devices when working with a topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, in the **Add node** drop-down list, select **New device**.

   A details area with the device settings appears in the right part of the window.

3. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.

4. On the **Address information** tab in the details area, specify the MAC and/or IP addresses of the device.

5. If additional address spaces were added to the application, specify the names of the address spaces for addresses.

6. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:

   - If you want to add an IP address, click **Add IP address**.
   - If you want to remove an IP address, click the icon located on the right of the field containing the IP address.

7. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To do so, perform one of the following actions:

   - If you want to add a network interface, click **Add interface** under the group of settings of the last network interface of the device.
   - If you want to delete a network interface, click the icon displayed to the right of the device network interface name (if there are two or more network interfaces).
   - If you want to define a different name for a network interface, click the icon located on the right of the current name and enter the new name for the network interface in the field that opens.

8. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the and icons. On the **Settings** tab, the and icons are located on the left side of the fields. On the **Address information** tab, the and icons are located to the right of the network interface name.

9. On the **Custom fields** tab in the details area, create a list of custom fields if needed.

10. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the icon.

The table of devices will show the new device with a status of *Authorized*.

Adding a device based on the node of an unknown device on the network interaction map

When working with the network interaction map, you can add a new device to the table of devices using a node representing a device that is unknown to the application.

To add a node of an unknown device to the table of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map** section, select the relevant node representing a device unknown to the application.

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

3. Click **Add to the devices table**.

   The details area will show the tabs for configuring the settings of the new device.

4. Configure the settings of the new device without changing the MAC- and/or IP address that are specified for the node.

   For a description of how to configure these settings, please refer to the procedure for manually adding a device when working with the table of devices.

5. Click **Save**.

The table of devices will show the new device with a status of *Authorized*. The node that previously represented a device that was unknown to the application will now represent a device on the network interaction map.

Adding a device based on an unmanaged switch on the topology map

When working with the topology map, you can add a new device to the table of devices using a node representing an unmanaged switch.

To add a node of an unmanaged switch to the table of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, select the relevant node that represents the unmanaged switch.

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

3. Click **Add to the devices table**.

   The details area will show the tabs for configuring the settings of the new device.

4. Specify the MAC address and/or IP address of the device and configure all other settings.

   For a description of how to configure these settings, please refer to the procedure for manually adding a device when working with the table of devices.

5. Click **Save**.

The table of devices will show the new device with a status of *Authorized*. The node that previously represented the unmanaged switch will now represent a known device on the topology map.

Merging devices

Industrial devices, as well as servers and workstations, may have multiple network interfaces used for redundancy or for operation in different network segments. The addresses of these network interfaces are usually used by devices at different times. Therefore, if these addresses are detected in traffic, the application may add multiple devices instead of just one device with different network interfaces. In addition, the application may not always match the IP and MAC addresses of one network interface of a device in traffic, which also causes separate devices with these addresses to be added to the table.

For such cases, the application provides the capability to merge devices. This allows you to get one device to control instead of multiple previously added devices. Devices can be merged automatically or manually. Devices can be automatically merged only when the Device Activity Detection method is enabled in learning mode and only under certain conditions, therefore devices can be merged only manually in a number of cases. You can merge devices when working with the devices table or when working with the network map.

To define the devices to be merged in the application, you can search for devices using the address information that is available in the accompanying documentation for your process control system (for example, in the detailed network design specifications or in the configuration of the HMI and PLC systems).

To merge several devices into one device, the total number of network interfaces in the new device must not exceed 512.

Users with any role except the Operator role can merge devices manually.

Merging devices when working with the table of devices

To merge devices in the table of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices that you want to merge.

4. Click **Merge devices**.

   The details area with the tabs for configuring the new device settings appears in the right part of the window.

5. Check the settings of the new device and edit them if necessary:

   - On the **Settings** tab in the details area, all fields containing conflicting values in the selected devices are marked by messages regarding the conflicting values. In this case, different values in text fields are merged into one value (for example, in the field containing the device name).

   - On the **Address information** tab in the details area, the MAC and IP addresses of the selected devices are distributed by individual network interfaces. If necessary, change the values of addresses, address spaces, and the names of network interfaces.

   - The list on the **Custom fields** tab in the details area contains all custom fields for the selected devices.

6. Check the specific device information for which you need to enable automatic updates again. Enable automatic updates for the necessary settings if they have been disabled.

   For example, you are advised to enable automatic updates for settings containing the values of the hardware and software versions on the device because these are the particular values that are used when detecting vulnerabilities of devices. Therefore, timely updates of such information are essential for risk management via the application.

   A setting with automatic updates disabled is designated by the icon. After enabling automatic updates, the setting is designated by the icon.

7. Click **Merge**.

   A window with a confirmation prompt opens.

8. In the prompt window, click **OK**.

The table of devices will show the new device with a status of *Authorized*.

Merging devices when working with the networking interactions map and the topology map

When working with the network interaction map, and the topology map, you can merge multiple nodes on the maps into one new device for the table of devices.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

WAN nodes cannot be merged.

To merge devices represented by nodes on the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Network map** section.

3. On the **Network interaction map** or **Topology map** tab, select several objects which represent nodes and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

4. Click **Merge devices**.

   The details area with the tabs for configuring the new device settings appears in the right part of the window.

5. Check the settings of the new device and edit them if necessary:

   - On the **Settings** tab in the details area, all fields containing conflicting values in the selected devices are marked by messages regarding the conflicting values. In this case, different values in text fields are merged into one value (for example, in the field containing the device name).
   - On the **Address information** tab in the details area, the MAC and IP addresses of the selected devices are distributed by individual network interfaces. If necessary, change the values of addresses, address spaces, and the names of network interfaces.
   - The list on the **Custom fields** tab in the details area contains all custom fields for the selected devices.

6. Check the specific device information for which you need to enable automatic updates again. Enable automatic updates for the necessary settings if they have been disabled.

For example, you are advised to enable automatic updates for settings containing the values of the hardware and software versions on the device because these are the particular values that are used when detecting vulnerabilities of devices. Therefore, timely updates of such information are essential for risk management via the application.

A setting with automatic updates disabled is designated by the icon. After enabling automatic updates, the setting is designated by the icon.

7. Click **Merge**.

   A window with a confirmation prompt opens.

8. In the prompt window, click **OK**.

The table of devices will show the new device with a status of *Authorized*. The network map will show one merged node instead of the previously selected multiple nodes.

Deleting devices

This section provides instructions on removing devices. You can delete one or multiple devices from the table of devices.

Users with any role except the Operator role can delete devices.

Information about deleted devices is not saved in the application. If deleted devices start displaying activity in the industrial network again, the application will add them to the table of devices as new devices, with a status of *Authorized* or *Unauthorized* depending on the current asset management mode.

Deleting devices when working with the table of devices

To delete devices from the table of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices that you want to delete.

4. Right-click to open the context menu of one of the selected devices.

5. In the context menu, select one of the following options:

   - **Delete device** if one device is selected.
   - **Delete devices** if multiple devices are selected.

   A window with a confirmation prompt opens.

6. If you have created Interaction Control rules for devices that include their address information, and you want to delete these rules at the same time, select the **Delete allow rules related to devices** check box.

7. In the prompt window, confirm deletion of the selected devices.

Removing devices when working with the networking interactions map and the topology map

When working with the network interaction map and the topology map, you can remove devices from the table of devices by using the nodes representing those devices on the maps.

To remove a device when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Network map** section.

3. On the **Network interaction map** or **Topology map** tab, select the node representing the device you want to remove.

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

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. If you have created Interaction Control rules for a device that include its address information, and you want to delete these rules at the same time, select the **Delete allow rules related to the device** check box.

6. In the prompt window, confirm deletion of the device.

Manually changing the statuses of devices

The application automatically assigns statuses to devices when monitoring the activity of devices in the industrial network. In some cases, you may need to manually change an automatically assigned device status. For example, this may be necessary if a device is required for industrial process support but this device was not active and was not added to the application when running in learning mode. When such a device is detected in monitoring mode, the application assigns the *Unauthorized* status to this device. The Unauthorized status can be changed only manually.

Users with any role except the Operator role can manually change the statuses of devices.

You can change the status (to *Authorized*, *Unauthorized*, or *Archived*) for one selected device or for multiple selected devices at once. If you are changing the status of one selected device, you can enable or disable automatic status changes to Archived for that device.

Cisco Switch connectors may automatically restrict network access for devices that have a status of *Unauthorized*. To avoid blocking necessary devices due to status changes, check the settings you defined for this connector type.

The application automatically changes the status of an *Archived* device if it shows activity. Depending on the current asset management mode, the application assigns a status of either *Authorized* or *Unauthorized* to the detected device.

Changing the statuses of devices when working with the table of devices

To change the status of devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Devices** tab in the **Assets** section.

3. In the devices table, select the devices whose status you want to change.

4. Open the **Change status** drop-down list in the toolbar.

5. In the drop-down list, select the command to assign the required status.

   A window with a confirmation prompt opens.

6. If you are assigning the *Authorized* status to devices and want to fine-tune the Interaction Control for these devices at the same time, select the check boxes for the relevant settings (the confirmation window displays the settings that are used when fine-tuning Interaction Control).

7. In the prompt window, confirm the change in the status of the selected devices.

Changing the statuses of devices when working with the networking interactions map and the topology map

When working with the network interaction map and the topology map, you can change the statuses of known devices represented by nodes on the maps.

You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To change the status of devices when working with maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Network map** section.

3. On the **Network interaction map** or **Topology map** tab, select the objects that represent nodes of known applications and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

4. Open the **Change status** drop-down list in the toolbar.

5. In the drop-down list, select the command to assign the required status.

   A window with a confirmation prompt opens.

6. If you are assigning the *Authorized* status to devices and want to fine-tune the Interaction Control for these devices at the same time, select the check boxes for the relevant settings (the confirmation window displays the settings that are used when fine-tuning Interaction Control).

7. In the prompt window, confirm the change in the status of the selected devices.

About arranging devices into groups

You can use the device group tree to arrange devices into groups. The device group tree supports up to six nesting levels.

Devices can be put into groups at any level of the hierarchy. However, each device can be added to only one of the groups in the tree.

The tree also has a limit of no more than 1000 groups.

Until a device is added to a specific group, information about this device does not contain any information about the specific location of the device. This device is assigned to the top level of the hierarchy within the group tree. After a device is added to a group, the application saves the location of this device as the full path to the group in the group tree.

Devices can be arranged into groups in the following ways:

- Automatically group devices based on a specific criterion.

  Using this type of device grouping, the application can automatically add groups to the device group tree. Groups are added when the application detects devices whose information matches the selected grouping criterion. The names of groups are assigned from a range of specific values for the selected criterion (for example, from the names of device categories when grouping by category).

- Manually arrange devices into groups.

  You can manually arrange devices into groups, including by adding devices into relevant groups and excluding them from other groups. When necessary, you can make changes to the device group tree by utilizing the available functions for manually forming the device group tree.

Automatic grouping of devices based on a specific criterion

This section contains instructions on automatically grouping devices by a specified criterion. You can automatically group devices in the device group tree based on one of the following criteria:

- Affiliation of IP addresses with subnets that are known to the application
- Device categories
- Device vendors

Users with any role except the Operator role can perform automatic grouping of devices.

Automatically grouping devices based on a specific criterion beginning with the top level of the hierarchy in the group tree

To automatically group devices by a specific criterion starting at the top level of the hierarchy in the group tree:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map** section, click one of the following buttons for selecting a grouping criterion in the toolbar located in the left part of the network interaction map display area:

   - – for grouping devices by subnet.
   - – for grouping devices by category.
   - – for grouping devices by vendor.

   A window opens with a prompt for you to select a grouping option.

3. To group devices by category and vendor based on address spaces, in the prompt window select the **Take into account the address spaces** check box.

4. Click one of the following buttons depending on your desired result:

   - To group devices by subnets, click **Group**.
   - To group devices by category and vendor based on address spaces in all groups of the device group tree, click **With child groups**.
   - To group devices by category and vendor based on address spaces only at the top level of the device group tree hierarchy, click **Selected group only**.

   The application will identify the devices that match the selected grouping criterion, create groups for these devices, and place the devices into these groups.

Automatically grouping devices in a selected device group:

To group devices automatically in a selected device group:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map**, select the group in which you want to automatically group devices.

3. Right-click to open the context menu.

4. In the context menu, select one of the following options:

   - **By subnet**.
   - **By category**.
   - **By vendor**.

   A window opens with a prompt for you to select a grouping option.

5. To group devices by category and vendor based on address spaces, in the prompt window select the **Take into account the address spaces** check box.

6. In the prompt window, click one of the following buttons depending on your desired result:

   - To group devices by subnets, click **Group**.
   - If you want to group devices by category or vendor in all child groups of the selected group, click **With child groups**.
   - If you want to group devices by category or vendor only in the selected group, click **Selected group only**.

   The application will identify the devices that match the selected grouping criterion, create groups for these devices, and place the devices into these groups (however, devices that are already in other groups will not be put into the new groups).

Manually arranging devices into groups

This section contains instructions on how to manually manage the placement of devices in the group tree. Users with any role except the Operator role can manage the placement of devices in the device group tree.

Add one device to a group

To add a device to a group in the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device to add to a group on both the network interaction map and the topology map.

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

3. Click **Edit**.

4. In the details area, go to the **Settings** tab.

5. Click the icon in the right part of the **Group** field.

   The **Select group in tree** window appears.

6. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.

7. Click **Select**.

   The path to the selected group will appear in the **Group** field.

8. Click **Save** in the details area.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the . icon.

Add multiple devices to a group

You can add multiple devices to a group when working with the table of devices.

When working with the network interaction map, you can also add multiple known devices represented by nodes on the map to a group. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To add multiple devices to a group when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices that you want to add to a group.

4. Right-click to open the context menu.

5. In the context menu, select **Group management** → **Move to group**.

   The **Select group in tree** window appears.

6. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.

7. Click **Select**.

   The path to the selected group will appear in the **Group** column.

To add multiple devices to a group when working with the network interaction map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map** section, select the relevant nodes of known devices and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

3. Right-click to open the context menu.

4. In the context menu, select **Move to group**.

   The **Select group in tree** window appears.

5. In the device group tree, select the relevant group.

   If the relevant group is not in the tree, you can add it in the currently open **Select group in tree** window.

6. Click **Select**.

   The selected nodes representing known devices will be displayed within the selected group.

Remove one device from a group

To remove a device from a group in the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device to remove from a group on both the network interaction map and the topology map.

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

3. Click **Edit**.

4. In the details area, go to the **Settings** tab.

5. In the **Group** field, delete the path to the group by clicking the × icon in the field (the icon is displayed if a group is defined).

6. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the . icon.

After saving the changes for the device, its **Group** value is cleared and the device will be assigned to the top level of the hierarchy within the group tree.

Remove multiple devices from groups

You can remove multiple devices from groups when working with the table of devices. The devices selected for removal from groups may be part of the same group or in different groups.

When working with the network interaction map, you can also remove multiple known devices represented by nodes on the map from groups. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To remove multiple devices from groups when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices that you want to remove from groups.

4. Right-click to open the context menu.

5. In the context menu, select **Group management → Remove from group**.

   A window with a confirmation prompt opens.

6. In the prompt window, confirm removal of the devices from groups.

For all selected devices, the **Group** value is cleared and these devices will be assigned to the top level of the hierarchy within the group tree.

To remove multiple devices from groups when working with the network interaction map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map** section, select the nodes in expanded groups and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

3. Right-click to open the context menu.

4. In the context menu, select **Remove from group**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm removal of the devices from groups.

For all selected devices, the **Group** value is cleared and these devices will be displayed outside of groups.

Moving nodes and groups to other groups on the network interaction map

You can change the location of nodes and groups in the device group tree by dragging objects on the network interaction map. After being moved, nodes and groups change their location in the device group tree just as when adding devices to a group and removing devices from groups.

Users with any role except the Operator 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 via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Network interaction map** tab in the **Network map** section, select the relevant nodes of known devices and/or collapsed groups.

To select multiple nodes and/or groups, do one of the following:

- Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
- Hold down the **CTRL** key and use your mouse to select the relevant objects.

3. Move the cursor over one of the selected objects (group or node representing a known device).
4. Press the **CTRL** key and hold it down while dragging the selected objects to the relevant group (or to any place outside of groups if you want to move the selected objects to the top level of the hierarchy within the group tree).

   A window with a confirmation prompt opens.
5. In the prompt window, confirm movement of the selected objects.

Manually creating a device group tree

You can create a device group tree when working with the table of devices, with the network interaction map and the topology map. Tree creation functions are available in the **Create group tree** or **Select group in tree** window.

Users with any role except the Operator role can create a device group tree.

To utilize the functions for creating a device group tree:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.
2. In the **Assets** section on the **Devices** tab or in the **Network map** section, do one of the following:

   - Open the **Create group tree** window by clicking **Configure groups**.

     In the **Assets** section, the **Configure groups** button is available in the **Group management** drop-down list in the toolbar.

     In the **Network map** section, the **Configure groups** button is only available on the **Network interaction map** tab.
   - Open the **Select group in tree** window while adding devices to groups. You can also open this window when filtering the table of devices by the **Group** column.

Any changes made to the device group tree in the **Create group tree** or **Select group in tree** window are applied immediately.

This section provides instructions on using the features for generating a device group tree.

Add group

To add a group to a device group tree:

1. In the **Create group tree** or **Select group in tree** window, add a new group in one of the following ways:
   - If the tree is empty and you want to add the first group, click **Add**, or press either **INSERT** or **ENTER**.
   - If you want to add a group on the same hierarchical level as an existing group, select this group and press **ENTER**.
   - If you want to add a child group to an existing group, select this group and click **Add** or press **INSERT**.
2. In the entry field, enter the group name.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   The group name must meet the following requirements:
   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of any other group included under the same parent group (not case-sensitive).
3. Click the ✓ icon on the right of the entry field.

Rename group

To rename a group in a device group tree:

1. In the **Create group tree** or **Select group in tree** window, select the group that you want to rename.
2. Click **Rename** or press **F2**.
3. In the entry field, enter the new name of the group.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _ /`.

   The group name must meet the following requirements:
   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of any other group included under the same parent group (not case-sensitive).
4. Click the ✓ icon on the right of the entry field.

The new group name will appear in the information about devices that are added to this group or to its child groups.

Deleting groups

When a group is deleted, the devices that were added to that group are not deleted. Instead, the devices from the deleted group are moved to the same level in the device tree hierarchy where the deleted group had been.

To delete a group from the device group tree:

1. In the **Create group tree** or **Select group in tree** window, select the group that you want to delete.
2. Click the icon.

   This opens a window prompting you to select a deletion option.
3. In the prompt window, click one of the following buttons depending on your desired result:

   - If you want to delete only the selected group and leave its child groups, click **Only the selected**.
   - If you want to delete the selected group together with all of its child groups, click **With child groups**.

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

Move group

To move a group within a device 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

You can find relevant groups in the device group tree by using the **Search groups** field in the **Create group tree** or **Select group in tree** window. Groups that meet the search criteria are displayed in the device group tree. For groups that are child groups, their parent groups are also displayed.

Update the tree

The composition of groups in the device group tree could be changed on the Server while you are working with the tree (for example, it could be changed by another user who is connected to the Server).

You can manually update the tree by using the icon in the **Create group tree** or **Select group in tree** window.

Adding and removing labels for devices

This section provides instructions on adding or removing device labels. You can assign any user-defined labels to devices.

A *device label* contains a text description that helps you quickly find or filter devices in the table. Any convenient text descriptions can be saved as labels. You can assign up to 16 labels for a device. Each device can have its own set of labels.

Lists of device labels are displayed in the table of devices in the **Labels** column. Labels in a cell are sorted in alphabetical order.

Users with any role except the Operator role can set and remove labels for devices.

Adding labels for one device

To set a label for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select a device for adding a label on both the network interaction map and the topology map.

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

3. Click **Edit**.

4. In the details area, go to the **Settings** tab.

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 device labels (not case-sensitive).
   - Contains from 1 to 255 characters.

6. If necessary, click **Copy labels** to copy the list of labels. The link is displayed if the list of labels is not empty.

7. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the . icon.

Adding labels for multiple devices

You can add labels for multiple devices when working with the table of devices.

When working with the network interaction map and the topology map, you can add labels for known devices represented by nodes on the maps. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To add labels for multiple devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to add labels.

4. Right-click to open the context menu of one of the selected devices.

5. In the context menu, select **Add labels**.

   The **Add labels** window opens.

6. In the **Labels** field, enter the text descriptions that you want to use as labels. To separate labels, you can use the **ENTER** key or the **;** character.

   You can use uppercase and lowercase letters, numerals, a space, and the following special characters: **! @ # № $ % ^ & ( ) [ ] { } ' , . - _**.

   A label name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Unique in the list of device labels (not case-sensitive).
   - Contains from 1 to 255 characters.

7. If necessary, click **Copy labels** to copy the list of labels. The link is displayed if the list of labels is not empty.

8. If you want to clear the current lists of labels for selected devices and provide only new labels for these devices, select the **Delete existing** check box.

   If the **Delete existing** check box is cleared, the current list of labels will remain on each device. The new labels will be added to the lists of labels on all selected devices. In this case, the total number of labels for some of the selected devices may exceed the limit (up to 16 labels for each device). The application checks this limit before adding new labels.

9. Click **OK**.

   The button is not available if the names of entered labels do not meet the requirements, or if the list of labels is empty while the **Delete existing** check box is cleared.

To add labels for multiple devices when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Network map** section.

3. On the **Network interaction map** or **Topology map** tab, select the relevant nodes of known devices and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

4. Right-click to open the context menu of one of the selected objects.

5. In the context menu, select **Add labels**.

   The **Add labels** window opens.

6. In the **Labels** field, enter the text descriptions that you want to use as labels. To separate labels, you can use the **ENTER** key or the `;` character.

   You can use uppercase and lowercase letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A label name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Unique in the list of device labels (not case-sensitive).
   - Contains from 1 to 255 characters.

7. If necessary, click **Copy labels** to copy the list of labels. The link is displayed if the list of labels is not empty.

8. If you want to clear the current lists of labels for selected devices and provide only new labels for these devices, select the **Delete existing** check box.

   If the **Delete existing** check box is cleared, the current list of labels will remain on each device. The new labels will be added to the lists of labels on all selected devices. In this case, the total number of labels for some of the selected devices may exceed the limit (up to 16 labels for each device). The application checks this limit before adding new labels.

9. Click **OK**.

   The button is not available if the names of entered labels do not meet the requirements, or if the list of labels is empty while the **Delete existing** check box is cleared.

Removing labels from one device

To remove a device label:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select a device for removing a label on both the network interaction map and the topology map.

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

3. Click **Edit**.

4. In the details area, go to the **Settings** tab.

5. In the **Labels** field, delete the labels that you no longer need:

   - If you want to delete specific labels, use the × icon next to the names of the labels.
   - If you want to delete all labels, use the × icon on the right side of the **Labels** field.

6. Click **Save**.

   This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the . icon.

Clearing lists of labels for multiple devices

You can clear the lists of labels for multiple devices when working with the table of devices.

When working with the network interaction map and the topology map, you can clear the lists of labels for known devices represented by nodes on the maps. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

To clear the lists of labels for multiple devices when working with the table:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to clear the lists of labels.

4. Right-click to open the context menu of one of the selected devices.

5. In the context menu, select **Add labels**.

   The **Add labels** window opens.

6. Select the **Delete existing** check box.

7. Click **OK**.

To clear the lists of labels for multiple devices when working with the maps:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Network map** section.

3. On the **Network interaction map** or **Topology map** tab, select the relevant nodes of known devices and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

4. Right-click to open the context menu of one of the selected objects.

5. In the context menu, select **Add labels**.

   The **Add labels** window opens.

6. Select the **Delete existing** check box.

7. Click **OK**.

Editing device information

Users with any role except the Operator role can edit device information.

To manually edit device information:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Devices** tab in the **Assets** section, select the relevant device.

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

3. Click **Edit**.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.

4. On the **Settings** tab in the details area, specify the relevant values in the fields that identify the device information.

5. On the **Address information** tab in the details area, specify the MAC and/or IP addresses of the device.

6. If additional address spaces were added to the application, specify the names of the address spaces for addresses.

7. You can specify multiple IP addresses for the same network interface of the device. To generate a list of IP addresses, perform one of the following actions:

   - If you want to add an IP address, click **Add IP address**.
   - If you want to remove an IP address, click the icon located on the right of the field containing the IP address.

8. If the device has multiple network interfaces, generate a list of network interfaces of the device and specify the corresponding MAC- and/or IP addresses for them.

   To generate a list of network interfaces of a device, perform one of the following actions:

   - If you want to add a network interface, click **Add interface** under the group of settings of the last network interface of the device.
   - If you want to delete a network interface, click the icon displayed to the right of the device network interface name (if there are two or more network interfaces).
   - If you want to define a different name for a network interface, click the icon located on the right of the current name and enter the new name for the network interface in the field that opens.

9. On the **Settings** and **Address information** tabs in the details area, enable or disable automatic updates for the relevant information about the device. To do this, use the and icons. On the **Settings** tab, the and icons are located on the left side of the fields. On the **Address information** tab, the and icons are located to the right of the network interface name. For the **Status** field, you can enable or disable automatic device status changes with the help of the icon.

10. On the **Custom fields** tab in the details area, create a list of custom fields and their values if necessary.

11. Click **Save**.

    This button is unavailable if not all required information is specified in the device settings or if invalid values have been defined. The tab containing settings requiring corrected values is marked by the icon.

After saving changes to device information, you can add or edit the Process Control settings for a device.

Adding, editing and deleting custom fields for a device

You can add, edit and delete custom fields containing information about devices. Custom fields are displayed in the details area when a device is selected.

For custom fields, the following limitations apply:

- The number of custom fields for one device shall not exceed 16.
- The number of characters in the field name can be no more than 100.
- The number of characters in the field value can be no more than 1024.

Users with any role except the Operator role can add, edit, and delete custom fields.

To add, edit, or delete a custom field:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Devices** tab in the **Assets** section, select the relevant device.

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

3. Click **Edit**.

   The details area displays the following tabs for viewing and editing the device information: **Settings**, **Address information**, and **Custom fields**.

4. Go to the **Custom fields** tab and perform one of the following actions:

   - If you want to add a custom field, click **Add custom field** and enter the name and value for the custom field in the fields that open.
   - 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**.

Deleting device users

When using device user monitoring, the application can automatically delete outdated accounts from the user table. Only the users whose data was previously received from the **External source** and **OVAL scanning** sources, but who are not present in the new data received from these sources, are automatically deleted.

If necessary, you can manually delete outdated accounts from the user table.

Users with the Administrator or Security Officer role can delete device user accounts.

To delete accounts from the user table:

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

2. Under **Assets** on the **Users** tab, select the user accounts that you want to delete.

3. Click **Delete**.

   A window with a confirmation prompt opens.

4. In the prompt window, click **OK**.

Removing device executable files

When launch control of executable files on devices is used, the application can automatically delete information about the files from the table of executable files. Automatic deletion occurs when the limit on the number or storage time of files is reached.

If necessary, you can manually delete outdated files from the table of executable files.

Users with the Administrator or Security Officer role can delete device executable files.

To remove files from the table of executable files:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. On the **Executable files** tab in the **Assets** section, select the files you want to delete.
3. Click **Delete**.

   A window with a confirmation prompt opens.
4. In the prompt window, click **Delete**.

Configuring address spaces

Kaspersky Industrial CyberSecurity for Networks monitors devices and their interactions while accounting for their address spaces (hereinafter also referred to as "AS"). *Address spaces* are intended for arranging addresses of devices into sets based on a specific attribute (for example, based on the specific network segments of devices).

Lists of rules and subnets are used to describe address spaces in the application.

An *address space rule* is a set of parameters that define the conditions for including addresses into a specific address space. To bind an address to an address space, each MAC or IP address must satisfy at least one address space rule. The application binds an address to the address space whose rule defines the most specific conditions for affiliation of this address (for example, if the address is explicitly specified in the rule).

Address space subnets are used to verify IP addresses detected by the application. Depending on the type of subnet that a detected IP address belongs to, the application may take different actions for asset management and device interaction control.

You can configure address spaces in the **Assets** section of the **Address spaces** tab. Each address space is presented as a data block containing information about the address space. This data block consists of a header and nested blocks containing tables of rules and subnets. When viewing information about address spaces, you can expand and collapse the contents of data blocks.

Default address space

By default, one shared address space named **Default** is defined in the application. This address space contains a single rule whose settings are configured to bind any MAC- and IP address to this specific address space. By default, the list of subnets of the **Default** address space contains a standard set of subnets that are most frequently used at organizations.

You cannot edit the rule of the **Default** address space or add other rules to this address space. However, users with the Administrator, Security Officer, or Infrastructure Officer role can edit the list of subnets in this address space to generate a set of subnets while taking into account the specific IP addressing of devices within the network of your organization. If Kaspersky Industrial CyberSecurity for Networks receives data from EPP applications, the application can use this data to automatically add subnets to the list of subnets.

Additional address spaces

If necessary, you can configure multiple address spaces in addition to the **Default** address space. You can generate user-defined rules and sets of subnets for added address spaces. Addresses that satisfy the conditions of the added address spaces will be bound to these address spaces. All other addresses will remain bound to the **Default** address space.

You may need to add address spaces when using devices that have identical addresses in different network segments, for example. In this case, after adding and configuring address spaces, the application will be able to distinguish address information based on additional attributes that the application will add to addresses in the form of address space names.

For examples of using address spaces, see the Appendices.

Binding addresses to address spaces

When using multiple address spaces, the application adds attributes containing the names of address spaces to all addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. Attributes containing the names of address spaces are no longer displayed for addresses if all added address spaces are deleted from the application (attributes of address spaces remain only for addresses in events and in certain risks associated with devices).

Attributes containing the names of address spaces denote the links between addresses and address spaces. Addresses that are bound to address spaces become dependent on these address spaces.

When deleting an address space that is bound to addresses, the application automatically deletes all addresses that are bound to the address space being deleted. These addresses are deleted from all application objects except events. When deleting an address from an object, the application checks for any other remaining addresses in this object. If there are no other remaining addresses, the application also deletes the object (such as a device).

About address space rules

The rules of address spaces are displayed in the **Rules** blocks within address space descriptions. Information about rules is displayed in the address space header and in the rules table.

The settings of address space rules are displayed in the following columns of the table:

- **Source**

  Type of source of incoming address information and list of selected data sources. The following types of data sources are available:

  - **Monitoring points** – monitoring points selected for the rule.
  - **Integration servers** – integration servers selected for the rule (the data on address information received from the selected integration servers will satisfy the address space rule).
  - **Active polling modules** – active polling module connectors selected for the rule (the data on address information received from the selected active polling modules will satisfy the address space rule).

  > The data sources must be specified in the address space rules after adding the objects to be used as sources to the application. For example, connectors for the **Active polling modules** data source must be specified after adding connectors of the **Active poll** type.

- **OSI model layers**

  Selected layers of the Open Systems Interconnection (OSI) model for an address space rule. A rule can be configured for addresses of the following OSI layers:

  - **Data Link (L2)** – MAC addresses.
  - **Network (L3)** – IP addresses.
  - **Data Link and Network (L2 and L3)** – MAC addresses and IP addresses.

- **VLAN ID**

  IDs of virtual local area networks (VLAN) that are applied when using VLAN technology in accordance with the IEEE 802.1q standard. When used for an address space rule, the **VLAN ID** may take the following values:

  - **Any are used** – VLAN technology is used for network interactions between devices, and any VLAN IDs can be used.
  - **Not used** – VLAN technology is not used for network interactions between devices.
  - **Any or not used** – VLAN technology is either not used for network interactions between devices, or it is used with any VLAN IDs.
  - **Fixed values** with a list of VLAN IDs – VLAN technology is used for network interactions between devices, and an address space can include only address information that has one of the listed VLAN IDs.

- **IP addresses**

  IP addresses included in the address space. Addresses can be specified individually, as ranges, or in CIDR subnet address format.

When viewing the rules table, you can use the configuration functions (by clicking the ⚙ icon) and search functions.

About address space subnets

The subnets of address spaces are displayed in the **Subnets** blocks within address space descriptions.

The application checks the detected IP addresses against the list of subnets of address spaces, and can do the following depending on whether the IP addresses belong to specific types of subnets:

- Add a device with its detected IP address to the table of devices and monitor the activity of this device.
- Display a device with its detected IP address on the network interaction map and the topology map as its corresponding type of node (known device, unknown device, or WAN node).
- Display a network interaction map link in which one of the sides of interaction is a device with a detected IP address.
- Verify the interaction of a device with a detected IP address based on defined rules (Interaction Control rules, Intrusion Detection rules, and correlation rules).
- Ignore the activity of a device with a detected IP address.

The settings of address space subnets are displayed in the following columns of the table:

- **Subnet**

  Subnet address in Classless Inter-Domain Routing (CIDR) format: `<base address of subnet>/<number of bits in mask>`. The addresses of subnets are displayed as a tree that shows the nesting hierarchy of subnets.

- **Type**

  Subnet type that determines its purpose. The following types are provided:

  - **Private, IT** – subnet for devices that serve as information technology (IT) resources, such as file servers.
  - **Private, OT** – subnet for devices relating to operating technologies (OT), such as PLCs.
  - **Private, DMZ** – subnet for devices that reside within a network segment of a demilitarized zone (DMZ), such as servers that handle requests from external networks.
  - **Public** – subnet that is considered to be an external (global) network for devices in other types of subnets. IP addresses from this subnet are represented by a WAN node on the network interaction map.
  - **Link-local** – subnet for network interactions within one segment of the local area network (not routed).

- **Range**.

  Range of IP addresses in the subnet.

- **Ignore MAC addresses**.

  Indicates whether detected MAC addresses are ignored when creating allow rules for network interactions involving IP addresses from the subnet. If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.

- **Automatically add subnets**.

  Indicates whether nested subnets are automatically added based on data received from EPP applications. If this mode is enabled, the application adds nested subnets based on data received from EPP applications.

When viewing the subnets table, you can use the configuration functions (by clicking the ⚙ icon), and the filter, search, and sorting functions.

Adding an address space

You can add address spaces to the application if you need to arrange addresses of devices into sets based on a specific attribute (for example, based on the specific network segments of devices).

Maximum number of address spaces in the application – 100.

Users with the Administrator, Security Officer, or Infrastructure Officer role can add address spaces.

To add an address space:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.

2. Select the **Assets** section.

3. On the **Address spaces** tab, open the details area by clicking **Add AS**.

4. Enter the name of the address space.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   The address space name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of another address space (not case-sensitive).

   > It is recommended to set an address space name that is no more than 6–8 characters long. If the name contains more characters, the address information may not be fully displayed in the cells of some data tables (for example, in the table of devices).

5. If necessary, enter a text description of the address space.

6. Configure the settings of the first address space rule.

7. If required, add and configure additional address space rules by clicking **Add rule**.

   The total number of rules in an address space cannot exceed 10.

8. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

The lower part of the **Address spaces** tab will show a separate block containing information about the added address space.

Generating a list of subnets for asset management

This section contains information about the features available for generating a list of subnets for asset management.

You can generate lists of subnets for address spaces while taking into account the specific addressing of devices within the network of your organization. This section provides instructions on using the features for generating a list of subnets.

If Kaspersky Industrial CyberSecurity for Networks receives data from EPP applications, the application can use this data to automatically add subnets in the appropriate address spaces. The application automatically adds detected subnets if they are nested within a subnet for which automatic addition of subnets is enabled.

Users with the Administrator, Security Officer, or Infrastructure Officer role can generate a list of subnets.

Adding a subnet

To add a subnet:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.

2. Select the **Assets** section.

3. On the **Address spaces** tab, expand the block containing information about the address space in which you want to add a subnet.

4. In the header of the **Subnets** block, click the + icon.

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

5. In the **Subnet** field, enter the subnet address in CIDR format: `<base address of subnet>/<number of bits in mask>`.

6. In the **Type** drop-down list, select the type of subnet according to its purpose.

7. Set the following toggle buttons to the necessary positions:

   - **Ignore MAC addresses for NIC rules** – enables and disables the mode for skipping detected MAC addresses when creating allow rules based on Network Integrity Control technology.

     If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.

   - **Automatically add subnets** – enables and disables automatic addition of nested subnets according to data received from EPP applications.

     If this mode is enabled, the application adds nested subnets within this subnet based on data received from EPP applications. By default, the type selected for the current subnet is indicated for these nested subnets.

8. Click **Save**.

The list of subnets will show the new subnet at its corresponding level of the hierarchy within the tree.

Editing subnet settings

To edit subnet settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.

2. Select the **Assets** section.

3. On the **Address spaces** tab, expand the block containing information about the address space in which you want to edit the subnet settings.

4. Expand the **Subnets** block and select the relevant subnet.

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

5. Click **Edit**.

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

   - In the **Subnet** field, enter the subnet address in CIDR format: `<base address of subnet>/<number of bits in mask>`.

     The address of the root subnet cannot be edited.

   - In the **Type** drop-down list, select the type of subnet according to its purpose.

     When changing the subnet type, keep in mind that a new type of subnet may affect the accessible operations that the application can perform with IP addresses from this subnet. For example, if you select the **Public** type, the network interaction map will no longer display links to devices that were assigned IP addresses from this subnet.

- Set the following toggle buttons to the necessary positions:

  - **Ignore MAC addresses for NIC rules** – enables and disables the mode for skipping detected MAC addresses when creating allow rules based on Network Integrity Control technology.

    If this option is enabled, the MAC addresses detected together with IP addresses from the subnet will not be added to Network Integrity Control rules in learning mode.

  - **Automatically add subnets** – enables and disables automatic addition of nested subnets according to data received from EPP applications.

    If this mode is enabled, the application adds nested subnets within this subnet based on data received from EPP applications. By default, the type selected for the current subnet is indicated for these nested subnets.

7. Click **Save**.

If the **Subnet** value is changed, the tree hierarchy level may be changed for a subnet.

Deleting subnets

In the list of subnets of an address space, you can delete any subnet except the root subnet in the tree (subnet 0.0.0.0/0).

To delete subnets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.

2. Select the **Assets** section.

3. On the **Address spaces** tab, expand the block containing information about the address space from which you want to delete subnets.

4. Expand the **Subnets** block and select the subnets to delete.

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

5. Click **Delete**.

   A window with a confirmation prompt opens.

6. In the prompt window, confirm deletion of the subnets.

Deleted subnets will no longer be displayed in the list of subnets. If a deleted subnet contained nested subnets, these subnets will remain in the list (but the tree hierarchy level of these subnets will change).

Viewing information about devices with IP addresses from the selected subnets

You can view information about devices with assigned IP addresses from the selected subnets in an address space. Information about devices is displayed in the table of devices. The table of devices automatically applies a filter based on the addresses of subnets.

To view information about devices in the table of devices:

1. Select the **Assets** section.
2. On the **Address spaces** tab, expand the block containing information about the address space containing the relevant subnets.
3. Expand the **Subnets** block and select the subnets for which you want to view information about devices.

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

The **Devices** tab opens in the **Assets** section. The table of devices will be filtered based on the IP addresses in the address information of devices.

Changing an address space

You can change the names, text descriptions, and settings of address space rules for added address spaces. These changes cannot be made to the **Default** address space.

You can also generate lists of subnets for any address spaces (including the list of subnets of the **Default** address space).

When changing the settings of an address space rule, you must take into account the established links between this address space and the addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. If changing the settings in address space rules results in the deletion of links between this address space and addresses, the application automatically deletes these addresses. This could lead to the deletion of application objects (such as devices) if these objects have no other remaining addresses.

Users with the Administrator, Security Officer, or Infrastructure Officer role can change the names, text descriptions, and settings of address space rules.

To change the name, text description, or settings of address space rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.
2. Select the **Assets** section.
3. On the **Address spaces** tab, click the icon in the block containing information about the relevant address space.

   The details area appears in the right part of the web interface window.
4. Depending on the necessary result, perform the following actions:

   - Enter the name of the address space.

     You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

The address space name must meet the following requirements:

- Must begin and end with any permitted character except a space.
- Must contain 255 characters or less.
- Must not match the name of another address space (not case-sensitive).

> It is recommended to set an address space name that is no more than 6–8 characters long. If the name contains more characters, the address information may not be fully displayed in the cells of some data tables (for example, in the table of devices).

- Enter a description of the address space.
- Configure the settings of address space rules.
- If necessary, add and configure additional address space rules by clicking **Add rule** or delete any unnecessary rules by using the × icons.

  The total number of rules in an address space cannot exceed 10.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

6. In the prompt window, confirm the changed address space settings.

Deleting an address space

You can delete address spaces that have been added. You cannot delete the **Default** address space.

> When deleting an address space, you must take into account the established links between this address space and the addresses that are indicated in application objects, including devices, risks, rules, events, and other objects. If deleting an address space results in the deletion of links between this address space and addresses, the application automatically deletes these addresses. This could lead to the deletion of application objects (such as devices) if these objects have no other remaining addresses.

Users with the Administrator, Security Officer, or Infrastructure Officer role can delete address spaces.

To delete an address space:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.
2. This action can be performed by a user with the Administrator, Security Officer, or Infrastructure Officer role.
3. Select the **Assets** section.

   On the **Address spaces** tab, click the 🗑 icon in the block containing information about the address space that you want to delete.

A window with a confirmation prompt opens.

4. In the prompt window, confirm deletion of the address space.

Configuring Process Control

Kaspersky Industrial CyberSecurity for Networks can monitor an industrial process by tracking process parameters and system commands transmitted in industrial network traffic. The application tracks this data for devices that are displayed in the table of devices and that have defined Process Control settings.

Process Control settings can be configured for the classes of devices and protocols that are supported by the application.

For automated control of the industrial process, you can employ Process Control rules and system command monitoring functionality. You can also track process parameters in real time.

A *Process Control rule* is a group of settings that define a condition for the values of a tag. Process Control rules contain descriptions of situations that must be detected in industrial network traffic (for example, when a tag exceeds the specified value).

When the condition defined in a rule is fulfilled, an event is registered by Kaspersky Industrial CyberSecurity for Networks. You can define the relevant event registration settings (for example, headers of events) when configuring Process Control rules.

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

Users with the Administrator, Security Officer, or ICS Officer role can configure Process Control settings for devices and generate lists of monitored tags and Process Control rules. The capability to view and export data is available to all users.

You can generate lists of monitored tags and Process Control rules on the Server web interface page in the **Process control** section. You can configure Process Control settings for devices when working with the devices in the **Assets** section and **Network map** section.

Supported devices and protocols

Kaspersky Industrial CyberSecurity for Networks analyzes traffic of the following classes of devices used for process automation:

- Programmable Logic Controllers (PLC):
  - ABB™ AC 700F
  - ABB AC 800M
  - ABB B&R
  - Allen-Bradley® ControlLogix® series

- Allen-Bradley CompactLogix™ series
- AutomationDirect DirectLOGIC
- BECKHOFF® CX series
- CHINT MAS400
- CHINT MAS9600
- Emerson DeltaV M series
- Emerson DeltaV S series
- Emerson ControlWave series
- General Electric RX3i
- Honeywell C300 for Experion PKS control systems
- Honeywell C300 for PlantCruise control systems
- Honeywell ControlEDGE 900 series
- IPU950
- Mitsubishi System Q E71
- OMRON CJ2M
- Schneider Electric Foxboro FCP270
- Schneider Electric Foxboro FCP280
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Schneider Electric Modicon Momentum
- Siemens SIMATIC® S7-200
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- YCU supporting the YARD protocol
- ELC supporting the YARD protocol
- Yokogawa CENTUM

- Yokogawa ProSafe-RS
- OWEN PLC100 series
- Prosoft-Systems Regul R500
- Tecon MFK
- KNX® devices
- Devices in Valmet DNA control systems
- Devices supporting the Allen-Bradley EtherNet/IP protocol
- Devices supporting the COS protocol
- Devices supporting the DTS protocol
- Devices supporting the FEU protocol
- Devices supporting the VNIIA protocol
- Devices supporting the PK4 protocol
- Devices supporting the PNU20 protocol
- Devices supporting the CODESYS V2 protocol
- Devices supporting the CODESYS V3 protocol
- Devices supporting the ISaGRAF protocols
- Devices supporting the Siemens S7comm protocol
- Devices supporting the Siemens S7comm-plus protocol
- Devices supporting PROFINET IO standard protocols

- Intelligent electronic devices (hereinafter referred to as IED):
  - ABB Relion™ REF615
  - ABB Relion RED670
  - ABB Relion REL670
  - ABB Relion RET670
  - General Electric Multilin B30
  - General Electric Multilin C60
  - MiCOM C264
  - Schneider Electric P545

    - Schneider Electric Sepam 80 NPP series
    - Siemens SIPROTEC™ 4 6MD66
    - Siemens SIPROTEC 4 7SA52
    - Siemens SIPROTEC 4 7SJ64
    - Siemens SIPROTEC 4 7SS52
    - Siemens SIPROTEC 4 7UM62
    - Siemens SIPROTEC 4 7UT63
    - Relematika TOR 300
    - EKRA 200 series
    - EKRA BE2502 series
    - EKRA BE2704 series
    - Devices supporting the DNP3 protocol
    - Devices supporting the Schneider Electric UMAS protocol
    - Devices supporting the IEC 60870-5-101 / IEC 60870-5-103 protocol
    - Devices supporting the IEC 60870-5-104 protocol
    - Devices supporting the IEC 61850-8-1 GOOSE protocol
    - Devices supporting the IEC 61850-8-1 MMS protocol
    - Devices supporting the IEC 61850-9-2 Sampled Values protocol
    - Devices supporting the Modbus TCP protocol
- Measurement devices:
    - Devices supporting the DLMS/COSEM protocol
- Devices with server software installed:
    - FTP server
    - OPC DA server
    - OPC UA server
    - Siemens SICAM PAS server
    - TASE.2 server

    - Server with encryption support
    - ARMS SCADA system devices
- Devices categorized as network equipment:
    - Moxa NPort series
    - I/O devices supporting the BACnet™ protocol
    - I/O devices supporting the FTP protocol
    - I/O devices supporting the IEC 60870-5-101 / IEC 60870-5-103 protocol
    - I/O devices supporting the IEC 60870-5-104 protocol
    - I/O devices supporting the Modbus TCP protocol
    - I/O devices supporting the OPC DA protocol, the WMI device interaction protocol
    - I/O devices supporting the OPC UA Binary device interaction protocol
    - Devices supporting Telnet control commands from the server

Kaspersky Industrial CyberSecurity for Networks also has *generic classes* of devices for process control: **Generic PLC**, **Generic IED** and **Generic Gateway**. Using these classes of devices, you can configure Kaspersky Industrial CyberSecurity for Networks to analyze traffic for those devices that are not on the list of supported classes. For generic classes of devices, you can specify any combination of application-level protocols from the list of supported protocols on devices related to programmable logic controllers, intelligent electronic devices and network gateways.

For the supported classes of devices, Kaspersky Industrial CyberSecurity for Networks analyzes communications over the following application-level protocols:

- ABB SPA-Bus
- Allen-Bradley EtherNet/IP
- BACnet
- BECKHOFF ADS/AMS
- BSAP
- CODESYS V2
- CODESYS V3 GATEWAY over TCP
- CODESYS V3 GATEWAY over UDP
- COS
- DLMS/COSEM
- DMS for ABB AC 700F devices

- DNP3
- Emerson ControlWave Designer
- Emerson DeltaV, including the protocol for updating embedded software (firmware)
- FTP
- General Electric EGD
- General Electric SRTP
- IEC 60870-5-101 / IEC 60870-5-103
- IEC 60870-5-104
- IEC 61850-8-1 GOOSE
- IEC 61850-8-1 MMS (including MMS Reports)
- IEC 61850-9-2 Sampled Values
- INA2000
- ISaGRAF IXL
- ISaGRAF SNCP
- KNXnet/IP
- Mitsubishi MELSEC System Q
- MMS (ISO 9506-2)
- Modbus TCP
- OMRON FINS over TCP
- OMRON FINS over UDP
- OMRON FINS over EtherNet/IP
- OPC DA, protocol for interaction of devices over WMI technology
- OPC UA Binary
- PROFINET DCP
- PROFINET IO
- RPC for PROFINET IO
- Schneider Electric UMAS
- Siemens S7comm

- Siemens S7comm-plus
- TASE.2 / IEC 60870-6
- TwinCAT3
- YARD
- Yokogawa Vnet/IP
- VNIIA
- Relematika BDUBus
- PK4
- PNU20
- Modification of the MMS protocol for ABB AC 800M devices
- Modification of the Modbus TCP protocol for EKRA 200 devices
- Automated radiation monitoring systems (ARMS) protocol
- Protocol for interaction between Siemens SICAM PAS and SICAM SCC (based on SIMATIC WinCC®)
- AutomationDirect DirectLOGIC device interaction protocol
- CHINT MAS400 device communication protocol
- CHINT MAS9600 device communication protocol
- Protocol for interaction of Foxboro FCP270 devices
- Protocol for interaction of Foxboro FCP280 devices
- IPU-FEU device interaction protocol
- MiCOM C264 device interaction protocol
- Valmet DNA device interaction protocol
- Protocol for initial setup of Prosoft-Systems devices
- Data Transfer Systems (DTS) protocol
- Protocol of devices with Siemens DIGSI 4 system software
- Protocols for interaction of devices in Honeywell Experion PKS / PlantCruise control systems
- Protocols for startup configuration and interaction of Moxa NPort series devices
- Protocols for detection and interaction of Honeywell ControlEDGE 900 series devices

To analyze traffic and interactions of devices, the application uses specialized modules for processing application-level protocols. The modules included in packages from the Kaspersky Industrial CyberSecurity for Networks distribution kit provide support for the listed classes of devices and application-level protocols. You can update protocol processing modules by installing updates. When installing updates to the application, new modules supporting additional classes of devices and/or application-layer protocols may be added.

Kaspersky Industrial CyberSecurity for Networks also analyzes traffic transmitted over common protocols. For a list of the supported common protocols, see the Appendix.

Process Control devices

For industrial process control purposes, you can use devices from the table of devices that have Process Control settings defined.

Kaspersky Industrial CyberSecurity for Networks supports the use of various classes of devices and application-layer protocols for Process Control.

You can view and edit Process Control settings in the details area of the device selected in the **Assets** section or in the **Network map** section of the Kaspersky Industrial CyberSecurity for Networks web interface.

Process Control settings for devices

Process Control settings for devices are displayed in the details area when a device is selected in the table of devices, on the network interaction map, or on the topology map. If the process control settings are set for the device, the **Process control** tab in the details area contains the following information:

- **Device class** – class of device from the list of device classes supported for Process Control.
- **Protocol** – name of the utilized protocol. The following information is displayed for each protocol:
  - **System commands** – main settings for tracking system commands for a protocol. This field shows the total number of system commands for the protocol and the number of monitored system commands that will cause the application to register events if detected.
  - Address information – depending on the selected protocol, this field contains the IP address and port, MAC address or domain ID (for the IEC 61850: GOOSE protocol). If additional address spaces were added to the application, the specific address space must be indicated for an address (and the OSI model layers selected for address space rules must match the address).
  - Additional settings depending on the selected protocol. Additional settings are displayed if the application lets you configure more than system commands and address information for this protocol.

Examples:
When the Modbus TCP protocol is selected, the additional setting **Reverse order of registers** is also displayed. This setting lets you enable or disable support for an inverted sequence of registers (machine words) in 32-bit data values.

When the IEC 60870-5-101 protocol is selected, the following additional settings are displayed:

- **Two-byte ASDU address** – lets you enable or disable two-byte addressing mode for application service data units (ASDU). If this mode is disabled, one-byte addressing is used.
- **Originator** – lets you enable or disable the use of an additional byte for the originator's address in the data block ID.
- **Channel address block (bytes)** – number of bytes in a data link layer address block.
- **Object address block (bytes)** – number of bytes in an information object address block.

You can add Process Control settings for devices in the following ways:

- Automatically
- Manually
- Import from external projects

About automatic detection of Process Control settings for devices

Kaspersky Industrial CyberSecurity for Networks can automatically identify the Process Control settings for devices and save these settings in the device information. Settings are identified by analyzing traffic to detect the protocol commands for devices involved in the industrial process.

The application automatically adds or edits Process Control settings for devices that have been added to the table of devices. Devices can also be automatically added to the table of devices if the Device Activity Detection method is enabled for Asset Management.

Automatically added Process Control settings are considered to be *system* settings. The application can change these settings if protocol commands with updated parameter information are detected in traffic.

Process Control settings that are manually added by a user are considered to be *custom settings*. The application does not change user-defined Process Control settings. If a user manually changes system settings for Process Control, these settings will also become custom settings.

Automatic detection of the Process Control settings for devices is performed when the Device Discovery for Process Control method based on the Deep Packet Inspection technology is used. You can enable and disable this method.

To automatically detect Process Control settings, the application employs modules for processing application-layer protocols. The application is installed with built-in modules that can determine the main settings for a number of devices and protocols that are indicated on the list of device classes and protocols supported by the application. You can update protocol processing modules by installing updates.

Manually adding Process Control settings for a device

You can manually add Process Control settings for a device when working with the table of devices, the network interaction map, or the topology map. Process Control settings that were added for a device are considered to be custom settings. User-defined settings are not changed when Process Control settings are automatically detected for devices.

Users with any role except the Operator role can add Process Control settings.

To add Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the relevant device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interaction map and the topology map.

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

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Add**.

   The **Add Process Control settings** window appears.

4. Configure the Process Control settings:

   a. Select the device class.

   b. Select the protocol used for interaction with the device within the industrial process.

   c. If necessary, edit the settings for monitoring system commands over the selected protocol. By default, the application monitors all system commands except those that are frequently encountered during normal operation of the device.

   d. If you need to configure other settings for the selected protocol (such as address information for interaction with the device), specify the relevant values in the fields that appear.

   e. If you want to additionally specify a different protocol (that is supported for the selected device class) or a different combination of settings for a previously selected protocol (when using multiple connected modules within one device), add the settings for this protocol by clicking the **Add protocol** link.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process control** tab, in the details area, a dedicated section with the specified settings is displayed.

Editing Process Control settings for a device

If Process Control settings were added for a device, you can manually edit these settings when working with the table of devices, the network interaction map, or the topology map. After saving the changes, Process Control settings for a device are considered to be custom settings. User-defined settings are not changed when Process Control settings are automatically detected for devices.

Users with any role except the Operator role can edit Process Control settings.

To edit Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the relevant device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interaction map and the topology map.

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

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Edit**.

   The **Edit Process Control settings** window appears.

4. Configure the Process Control settings. You can edit individual settings (for example, edit the settings for tracking system commands for a specific protocol) or reconfigure all settings in the same order as you would when adding Process Control settings.

   When you edit settings that were used in previously created tags, the application automatically deletes these tags and their associated Process Control rules. For example, if you delete a protocol, after saving the settings the application will delete all tags containing the device and deleted protocol (the Process Control rules associated with these tags will also be deleted).

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process control** tab, in the details area, the information in the section with the previously defined settings is refreshed.

Selecting the monitored system commands

You can configure traffic monitoring of system commands that are transmitted and received by process control devices.

In Kaspersky Industrial CyberSecurity for Networks, system commands include management commands (for example, START PLC) as well as system messages related to the operation of devices or containing packet analysis results (for example, REQUEST NOT FOUND). System commands in Kaspersky Industrial CyberSecurity for Networks are categorized based on the categories listed in the Appendices.

When a monitored system command is detected, Kaspersky Industrial CyberSecurity for Networks registers an event for Command Control technology. The event is registered using the system event type that is assigned the code 4000002602. You can configure the settings for this type of event.

Users with any role except the Operator role can configure system command monitoring for devices.

To configure monitoring of system commands for a device:

1. In the **Assets** section on the **Devices** tab or in the **Network map** section, select the relevant device with defined Process Control settings.

   In the **Network map** section, you can select the device on both the network interaction map and the topology map.

   If Process Control settings are not defined for a device, add the settings.

2. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Edit**.

   The **Edit Process Control settings** window appears.

3. Specify the relevant system commands for the first protocol. To do so, expand the **System commands** list under the **Protocol** field and select the check boxes of the system commands that you want to monitor. After selecting system commands, click **OK**.

4. If a different protocol is additionally indicated in the Process Control settings, or if it is the same protocol but with different address information, select the system commands that will be monitored during communications over this protocol. To do so, use the **System commands** drop-down list under the field containing the name of this protocol. Likewise, configure monitoring of system commands for all other specified protocols of the device.

5. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

On the **Process control** tab, in the details area, the information in the section with the previously defined settings is refreshed.

Clearing Process Control settings defined for a device

You can clear Process Control settings for a device when working with the table of devices, the network interaction map, or the topology map.

When clearing Process Control settings defined for a device, the application automatically deletes all tags that were created for this device. In addition to the tags, all of their associated Process Control rules are also deleted.

Users with any role except the Operator role can clear Process Control settings for devices.

To clear Process Control settings for a device:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the relevant device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the relevant device on both the network interaction map and the topology map.

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

3. In the upper right corner of the details area, click the ⋮ icon and select **Process Control settings** → **Delete**.

   A window with a confirmation prompt opens.

4. In the prompt window, confirm deletion of the settings.

The Process Control settings section is deleted from the **Process control** tab in the details area.

Importing configurations of devices and tags from external projects

Configurations of Process Control settings for devices and tags can be imported into Kaspersky Industrial CyberSecurity for Networks from external project files. In the context of Kaspersky Industrial CyberSecurity for Networks, *external projects* are projects that contain data on devices and tags saved by other systems (such as a SCADA system).

To import files of external projects, the files must be packed into a ZIP archive (except for files of certain projects whose contents consist of a ZIP archive). You can import device and tag configurations only from files belonging to supported external project types.

You can update and expand the supported types of projects by installing updates.

To import configurations of devices and tags from an external project:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

   On the **Devices** tab in the toolbar above the table of devices, open the **Import** drop-down list.

3. In the drop-down list, select the option with the relevant project type.

   The **Importing <project type>** window will appear on the screen.

4. In the **File to import** field, select the project file by clicking **Browse**.

5. Select the relevant option for your existing configurations of devices and tags. To do so, click one of the following buttons:

   - **Add** – to add the imported device configurations and tags are added to the existing device configurations and tags.

   - **Replace** – to import the new device configurations and tags and delete the pre-existing configurations and tags associated with the devices for which you import new configurations and tags (tags with user-defined process control rules are not deleted).

6. Confirm the import by clicking **Continue**.

   The data import process starts. Information about the running import operation is displayed in the list of background operations. When the process completes, the imported configurations of devices and tags will be available for upload in the table of devices and table of tags.

7. If you want to view a report on the results of the import:

   a. Click in the application web interface menu.

      The list of background operations opens.

   b. Wait for the import operation to complete.

   c. Click **Display report**.

Supported types of projects for importing

Configurations of devices and tags can be imported from data files comprising the following types of projects:

- Universal-format project.

  This type of project can be obtained from any source by converting and saving its data in text files with delimiters in CSV format. For information about files in a universal project, please refer to the Appendices.

- AC 800M configuration file for OPC server.

  This type of project can be obtained via ABB AC 800M device management software.

- Control Builder M project.

  This type of project can be obtained via ABB Control Builder M software.

- COS device configuration archive.

  This type of project can be obtained via device management software for devices supporting the COS protocol.

  > Configuration files of devices do not contain the network IP addresses that are used by these devices. After adding devices from configuration files, you will need to verify the information about devices in the application and manually define the correct IP addresses for these devices if necessary.

- DeltaV project.

  This type of project can be obtained via Emerson DeltaV device management software.

- DirectSOFT6 project.

  This type of project can be obtained via DirectLOGIC device management software.

- ABB Freelance 2016 Engineering tag list.

  This type of project can be obtained via ABB Freelance 2016 Engineering software.

- Project for IEC 61850 devices.

  This type of project can be obtained via device management software for devices supporting IEC 61850 standard protocols.

  > Imports of SCD, CID, and ICD file types prepared in accordance with the IEC 61850-6 standard are supported. For more information about the application's capabilities in terms of processing and managing the configurations saved in these files, see the Appendix.

- RSLogix 5000® project (provided as a CSV- or ACD file).

  This type of project can be obtained via RSLogix 5000 device management software.

  > When importing a CSV file containing an RSLogix 5000 project, the application ignores structural and custom types of tags in this project. If you want to add these tags to the application, you can import an ACD file containing the RSLogix 5000 project or enable Unknown Tag Detection to add tags from traffic.

- SICAM PAS V7 project (represented by a description TXT file or a PXD file).

  This type of project can be obtained via Siemens SICAM PAS version 7 software.

- TIA Portal V12/V13 project.

  This type of project can be obtained via Siemens TIA Portal version 12 or 13 software.

- Schneider Electric Unity project.

  This type of project can be obtained via Schneider Electric Modicon device management software. A project can be provided as ZEF or XEF files (if a project is provided as a ZEF file, this file does not need to be packed into a ZIP archive for import).

  When a Schneider Electric Unity project is imported, the added devices are assigned the names of the files from which they were imported. You can manually define names for these devices when editing device information.

- WinCC project (including WinCC OA, WinCC flexible).

  This type of project can be obtained via Siemens SIMATIC WinCC, WinCC OA, or WinCC flexible software.

- YARD configuration file.

  This type of project can be obtained via device management software for devices supporting the YARD protocol.

- CIMPLICITY export CSV file.

  This type of project can be obtained via CIMPLICITY software.

- Valmet DNA configuration file.

  This type of project can be obtained via Valmet DNA software.

- EGD configuration XML file.

  This type of project can be obtained by exporting a configuration for data exchange via the General Electric EGD protocol.

- ControlWave project SIG-file.

  This file is included in the project used by Emerson ControlWave series devices.

- Honeywell Control Builder project.

  This type of project can be obtained via Honeywell Control Builder software.

- PcVue V10/V11 project

  This type of project can be obtained via PcVue version 10 or 11 software.

- Proficy export CSV file.

  This type of project can be obtained via Proficy software.

- Foxboro IACC export file project.

  This type of project can be obtained via Foxboro IACC software.

- PNU20 configuration file.

  This type of project can be obtained via device management software for devices supporting the PNU20 protocol.

- CHINT MAS400 project.

  This type of project can be obtained via the CHINT MAS400 device management software.

- CHINT MAS9600 project.

  This type of project can be obtained via the CHINT MAS9600 device management software.

- XWS file with ISaGRAF project debug information.

  This type of project can be obtained via device management software for devices supporting the ISaGRAF protocols.

- CSV files.

  This type of project can be obtained from any sources supporting export of device information as a CSV file. The data in the CSV files must be presented as records in the same format as the device data CSV files exported from Kaspersky Industrial CyberSecurity for Networks.

Tags

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

You can add tags to the application in the following ways:

- Manually
- Automatically when unknown tags are detected
- Importing from external projects

A tag can be added under the following conditions:

- The table of devices contains a device associated with the tag being added.
- A device has defined Process Control settings in which the protocol of the added tag is indicated.

After adding a tag to the application, this tag can be used in Process Control rules. In accordance with the conditions defined in Process Control rules, the application will register the corresponding events in which the received tag values may be saved.

You do not need to add this tag to Process Control rules to control tag values when monitoring process parameters.

You can view and edit tags in the **Process control** section of the **Tags** tab.

About Unknown Tag Detection

Kaspersky Industrial CyberSecurity for Networks can analyze traffic to detect and save information about unknown tags. Unknown tags are tags that are absent from the table of tags.

The application adds a detected tag to the table of tags if the conditions for adding a tag are fulfilled. If one of the conditions is not fulfilled, the detected tag is ignored (for example, if the tag has no associated protocol specified for the device in the Process Control settings).

Information about unknown tags is received from traffic using the Unknown tag detection method based on the Deep Packet Inspection technology. You can enable and disable this method.

When the Unknown Tag Detection method is used, the performance of application-layer protocol processing modules may be slightly reduced. For this reason, Unknown Tag Detection is disabled by default after the application is installed. It is recommended to enable the Unknown Tag Detection method for a period of time sufficient to detect all tags that may be associated with devices with the specified Process Control settings. It is recommended to disable this method after the detected tags are added to the table.

Unknown Tag Detection is supported for the following protocols:

- Allen-Bradley EtherNet/IP
- BACnet
- BSAP
- CODESYS V3 Gateway
- DMS for ABB AC 700F devices
- DNP3
- Emerson DeltaV
- IEC 60870: IEC 60870-5-101, IEC 60870-5-104
- Modbus TCP
- OPC DA
- OPC UA Binary
- Schneider Electric UMAS
- Siemens S7comm
- TASE.2
- Yokogawa Vnet/IP
- PNU20
- Protocol for interaction of Foxboro FCP270 and FCP280 devices

Manually adding a tag

Users with the Administrator, Security Officer, or ICS Officer role can manually add tags.

To manually add a new tag:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Tags** tab, open the details area by clicking **Add tag**.

4. Click **Select device** to open the device selection window.

5. In the device selection window, select the device for which you want to create a tag and click **OK**.

   The device selection window contains a table in which you can configure the layout and order of columns, and also filter, search, and sort similarly to the table of devices in the **Assets** section.

6. Select the protocol that is indicated in the Process Control settings for the selected device. You must select a protocol supporting the transmission of tags.

   If the necessary protocol is not available, you can configure the Process Control settings and specify the necessary protocol. To open the settings window, use the button on the right of the protocol selection field. Process Control settings are configured the same as when adding or editing settings while working with the table of devices.

7. Change the tag name if necessary. The default name according to the template is **Tag <value of the device tag counter>**.

   You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The tag name must begin and end with any permitted character except a space.

8. Configure other tag parameters.

   The mandatory parameters (such as the tag name and data type) must be specified for a tag. Depending on the selected protocol and data type, additional parameters (such as the unit of measure and scaling limits) may be available for configuration.

9. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

The new tag appears in the table of tags.

Editing tag parameters

Users with the Administrator, Security Officer, or ICS Officer role can edit tag settings.

To edit tag settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Tags** tab, select the relevant tag.

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

4. Click **Edit**.

5. Change the tag name if necessary.

   You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The tag name must begin and end with any permitted character except a space.

6. Configure other tag parameters.

   The mandatory parameters (such as the tag name and data type) must be specified for a tag. Depending on the selected protocol and data type, additional parameters (such as the unit of measure and scaling limits) may be available for configuration.

7. Click **Save**.

   This button is unavailable if not all required values are specified or if there are invalid values in the settings.

Adding tags to the favorites list

If you want to create a list of the most important tags and quickly navigate to this list (for example, to view the current values of these tags), you can add tags to the favorites list. Tags can be added to the favorites list and deleted from it at your own discretion. The number of tags on the favorites list is unlimited.

To display the list of favorite tags, you can filter by the **Favorites** column when viewing the table of tags.

A created tag is not add to the favorites list by default.

To add tags to the favorites list:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Tags** tab, select the tags that you want to add to the favorites list.

4. Right-click to display the context menu of one of the selected tags.

5. In the context menu, select **Add to favorites list**.

In the table of tags, **True** is displayed for all selected tags in the **Favorites** column.

To delete tags from the favorites list:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Tags** tab, select the tags that you want to remove from the favorites list.
4. Right-click to display the context menu of one of the selected tags.
5. In the context menu, select **Remove from favorites list**.

In the table of tags, **False** is displayed for all selected tags in the **Favorites** column.

Deleting tags

Users with the Administrator, Security Officer, or ICS Officer role can delete tags.

To delete tags:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.
2. Select the **Process control** section.
3. On the **Tags** tab, select the tags that you want to delete.
4. In the toolbar above the table of tags, click **Delete**.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the tags.

Process Control rules

The application can employ the following Process Control rules to monitor the values of tags:

- Rules with defined conditions. These rules contain conditions for tracking the values of tags. Each rule can contain one of the provided types of conditions. If a condition defined in a rule is fulfilled, the application registers an event. The settings of a registered event are also defined in the rule.
- Rules with Lua scripts. These rules contain descriptions of algorithms used for checking the values of tags. The algorithms are compiled in the Lua programming language using functions and variables for Lua scripts. When an algorithm in a rule containing a Lua script is triggered, the application registers an event (the settings of a registered event are defined in the rule). If you are using Lua scripts for Process Control rules, you can use a *global Lua script* that initializes the global Lua variables and functions. You can use these global variables and functions in a Lua script of any rule. By default, the global Lua script is empty and does not contain executable code. The application can have only one global Lua script at one time.

The application applies Process Control rules when using the rule-based process control method based on the Deep Packet Inspection technology. You can enable and disable this method.

Process Control rules can be enabled or disabled. Enabled rules are applied during traffic analysis. Disabled rules are not applied and are not taken into account.

The application can automatically create Process Control rules with defined conditions when Process Control is running in learning mode.

You can view and edit Process Control rules in the **Process control** section on the **Rules** tab.

Rules with defined conditions for tag values

To monitor the values of tags, you can employ Process Control rules in which conditions are defined for the values of tags. Each rule can contain one of the provided types of conditions. A rule can be bound to only one tag. However, you can create up to 20 rules with different types of conditions for one tag.

Rules with defined conditions can be created automatically by the application when Process Control is running in learning mode. You can also manually create and edit rules with defined conditions for the values of tags.

For a Process Control rule, you can select one of the following types of conditions:

- **Value changed** – the value of the controlled tag was either completely changed or was changed in a specific bit.

  If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of any type of tag. You can also specify the number of saved (allowed) values of a tag whose detection will not result in the registration of an event. For a rule, you can specify a number of saved values from 1 to 10 (the saved values will be updated as new values are detected). By default, only the latest value is saved.

  If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64).

- **Tag missing** – the controlled tag was not detected in monitored traffic during the defined time period.

  You can use this condition to monitor any type of tag.

- **Detection** – the controlled tag was detected in the traffic being monitored.

  You can use this condition to monitor any type of tag.

- **In range** – the value of the controlled tag is inside the specified range.

  You can use this condition to monitor only int and float tags.

  You can define values for the lower and/or upper limit of the range. The defined values for limits can be included in the range or excluded from it.

- **Out of range** – the value of the controlled tag is outside of the specified range.

  You can use this condition to monitor only int and float tags.

  You can define values for the lower and/or upper limit of the range. The defined values for limits can be included in the range or excluded from it.

- **Equals** – the value of the controlled tag is equal to one of the defined values, either completely or in a specific bit.

  If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of int, bool and string tags. You can define from 1 to 10 values for comparison.

  If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64) and the value of the bit for comparison (indicated as one of two integers: zero or one).

- **Does not equal** – the value of the controlled tag is not equal to one of the defined values, neither completely nor in a specific bit.

If a particular bit of a value is not being specifically monitored, you can use this condition to monitor the value of int, bool and string tags. You can define from 1 to 10 values for comparison.

If a particular bit of a value is being specifically monitored, you can use this condition to monitor only int and unsigned int tags. For monitoring purposes, you need to specify the sequence number of the monitored bit in the tag (integer within the range corresponding to the data type of the selected tag: from 1 to 8, 16, 32 or 64) and the value of the bit for comparison (indicated as one of two integers: zero or one).

- **Monotonic change violation** – the value of a controlled tag violates the sequence of monotonic increase or reduction of values.

  You can use this condition to monitor only int and float tags.

For rules that monitor the values of tags, you need to take into account how the application processes values represented by denormalized numbers (low-order numbers approaching zero – for example, 2.22507e-308 if this value is represented with double precision). The application converts denormalized numbers into zero values.

For any condition, you can select the operations for which the application will monitor the values of a tag. The following monitoring options are available depending on operations performed with the tag:

- **Monitor when reading tag** – the value is checked when reading a tag from a device.
- **Monitor when writing tag** – the value is checked when writing a tag to a device.

Rules with Lua scripts

Scripts written in the Lua programming language can be used to describe the algorithms for checking the values of tags in Process Control rules. Lua scripts provide the capabilities to not only check the values of tags but also to add various information to registered events and process logs.

A Lua script must consist of one or more functions. The names of the functions must be unique among all rules with Lua scripts. A function that is used to track the values of tags is called a *trigger function*. A trigger function must return a value of `true` to register an event.

If a variable is indicated in a script, the variable must be initialized either in that specific script (to be applied only in that script) or in a separate global script (to be applied in all rules with Lua scripts). A global script can also contain auxiliary functions that can be used in rules with Lua scripts.

A trigger function is called whenever the value of any tag used in the function is changed. The function is first called when all values of tags used in the function are received.

To obtain the values of a tag, the code of a function contains an entry that looks as follows:

```
tag'main_tag_parameters[:field_name][@modifier]'[.transmission_direction]
```

where:

- `main_tag_parameters` are the mandatory parameters that identify the tag in the application. The main parameters consist of the following parameters from the table of tags:

  - **Device**

    This parameter is separated from the next one by a colon (`:`).

- **Tag name**

  This parameter is separated from the next one by a slash (`/`).

- **Tag ID**

- `field_name` is the name of the field within the tag field structure defined in **Structural values**, in the table of tags. If a field is embedded into other fields, its name is indicated together with the names of all parent fields separated by a colon. If the `field_name` parameter is not specified, the main value within the tag field structure is checked.

- `modifier` determines how the data is represented and obtained. The following modifiers are available:

  - `type` means that the passed value is the data type of the obtained value.

  - `str` means that the obtained value is converted into a string value.

  - `loc` means that the passed value is the assigned localized name for the obtained value (if there is no localized named, the obtained value is converted into a string value).

  - `ts` is used to get the timestamp of the last tag value update (UTC, in microseconds starting on 1970.01.01). The modifier is not applied to fields.

  If a modifier is not specified, the actual obtained value is used. In this case, the data type of the value is not changed.

- `transmission_direction` defines the direction in which the obtained value is transmitted. The transmission direction can be defined by one of the following parameters:

  - `r` means that the value was received when it was read from a device.

  - `w` means that the value was received when it was written to a device.

  - `rw` refers to any direction of the obtained value.

  If the transmission direction is not defined, the value obtained from any direction is used.

Example

```
tag'BayController:BayControllerQ.T1MMXU1.PhV.phsA/73:cVal:mag:f'
```

where:

- `BayController` is the device name.

- `BayControllerQ.T1MMXU1.PhV.phsA` is the tag name.

- `73` is the tag ID.

- `cVal:mag:f` is the field name combined with the names of the parent fields.

Records for obtaining the values of tags can be used in expressions (for example, assigning values to variables or comparing values).

To perform various operations with a Lua script, you can use *auxiliary functions* supported by the Server. The names of auxiliary functions begin with an underscore (_).

The main auxiliary functions for adding information via Lua scripts are as follows:

- Function for adding parameters to use as additional variables in events:

  ```
  _AddEventParam('parameter_name', parameter_value)
  ```

  Any name and value can be defined for a parameter. To use a parameter and its value in events, this parameter must be specified in event type parameters as `$extra.<parameter_name>`.

- Functions for adding entries to the process log in which the Lua script is executed (this is normally a process whose name starts with the word `Filter`). A record defined by an argument of the function (variable or constant) is added to the log:

  - To create a record with the *Errors* level:

    ```
    _WriteErrorLog(function_argument)
    ```

  - To create a record with the *Warning* level:

    ```
    _WriteWarningLog(function_argument)
    ```

  - To create a record with the *Info* level:

    ```
    _WriteInfoLog(function_argument)
    ```

  - To create a record with the *Debug* level:

    ```
    _WriteDebugLog(function_argument)
    ```

  - To create a record with the *Debug* level that may contain multiple arguments of the function:

    ```
    print(function_argument1, function_argument2,…)
    ```

    Variables or constants defined by function arguments are separated by a tab character in a log record.

  Records are not created in the log if the level of the record is lower than the logging level set for the process.

Process Control rules learning mode

To reduce the number of same-type actions and to automate the process of creating and configuring rules, the application uses machine learning methods and baseline models. The application analyzes various patterns in the changing tag values that are detected during traffic processing and generates ready-to-use Process Control rules. Machine learning methods are used when rules learning mode is enabled.

In Process Control rules learning mode, the application automatically generates Process Control rules with conditions for the values of tags. To generate rules, the application analyzes traffic to monitor the values of only those tags that have been added to the table of tags.

Process Control rules that were automatically added in learning mode are called *system* rules. For these rules, **Source** is set to **System**. When system rules are automatically created, **Event score** is set to 6.0 by default.

Rules that were manually created are called *User* rules. For these rules, **Source** is set to **User**. If a system rule is manually changed, this rule also becomes a user rule.

The application assigns a status of *Disabled* to rules added in learning mode. If a system rule was updated in learning mode, this rule retains its status before the update: *Enabled* or *Disabled*.

When adding or updating Process Control rules in learning mode, the application defines one of the following conditions for them:

- **Does not equal**.

  This condition is defined when a rule is added if no other system rule is found for the detected tag value or if up to ten different tag values are received (except for the tags with the bool or float data type).

- **Out of range**.

  This condition replaces the previous condition in a rule if a new value for a tag with the float data type is received or if more than ten different values for a tag with the int data type are received.

- **Monotonic change violation**.

  This condition replaces the previous condition in a rule if the detected tag values have only increased or only decreased, without any other variation. This condition replaces the previous condition in rules for tags with the int or float data type when learning mode ends.

In learning mode, the application also deletes system Process Control rules in the following cases:

- The rule was created for a tag with the bool data type, and the detected and saved values do not match (comparisons are conducted only for the first ten detected values, and all other values are ignored).

- The rule was created for a tag with the string data type, and more than ten different values are received.

You can configure the learning mode for the rule-based process control method.

Process Control rules learning mode must be enabled for a sufficient amount of time to detect all possible values of relevant tags. This amount of time depends on how frequently tags are circulated in traffic, how often devices are running in the industrial network, and other specifics of the industrial process. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period ranging from one to several days to accumulate the maximum amount of data.

Viewing the table of Process Control rules

The Process Control rules table is displayed in the **Process control** section on the **Rules** tab. The table provides the general settings of rules and of the tags and devices associated with the rules.

The settings of rules are displayed in the following columns of the table:

- **Rule ID**

  Unique ID of the rule.

- **Device group**

  Name of the group containing the device associated with the tag (contains the name of the group and the names of all its parent groups in the device group tree).

- **Device**

  Name of the device associated with the tag.

- **Protocol**

  Name of the protocol used to transmit the tag.

- **Tag name**

  Defined name of the tag for which the rule was created.

- **Rule**

  Defined name of the rule.

- **Rule description**

  Defined description of the rule.

- **Status**

  Current status of the rule (*Enabled* or *Disabled*).

- **Created**

  The date and time when the rule was created.

- **Changed**

  The date and time when the rule was last modified.

- **Condition type**

  Selected type of condition for the rule.

- **Event title**

  Header of the event registered when the rule is triggered.

- **Event score**

  Assessed score of the event that was registered when the rule was triggered. Events are scored on a scale from 0.0 to 10.0.

- **Event description**.

  Description of the event registered when the rule is triggered.

- **Source**

  Information about the origin of the rule.

When viewing the rules table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Creating a Process Control rule with settings of conditions

The following options are provided for creating Process Control rules with settings of conditions:

- Create a new rule for a tag.
- Create an additional rule based on an existing rule.

To create a new rule for a tag:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.
3. On the **Tags** tab, select the tag for which you want to create a Process Control rule.

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

4. In the upper right corner of the details area, click **Create rule**.

   This opens the **Rules** tab containing the details area for the created Process Control rule.

5. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

      You can use letters of the English alphabet, numerals, and the following special characters: `( ) . , : ; ? ! * + % - < > @ [ ] { } / \ _ $ #`. The rule name must begin and end with any permitted character except a space.

   c. Select the type of condition and configure the settings depending on the selected type.

   d. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).

6. Click **Save**.

To create an additional Process Control rule based on an existing rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.
3. On the **Rules** tab, select the rule that you want to use as the basis for creating another rule for the same tag.

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

4. Click **Create new rule**.

   You will see the details area for the created Process Control rule. For the new rule, you will see information about the device, protocol and tag received from the settings of the selected rule.

5. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

   c. Select the type of condition and configure the settings depending on the selected type.

   d. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).

6. Click **Save**.

Creating a Process Control rule with a Lua script

To create a rule with a Lua script:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Rules** tab, open the details area by clicking **Add Lua script**.

4. Perform the following actions:

   a. Use the **Enable** toggle to define the status of the rule: *Enabled* or *Disabled*.

   b. Enter the rule name and description.

   c. In the **Lua script for rule** field, enter the code of the script in the Lua language.

      When entering text, suggestions or available values automatically appear near the cursor (for example, relevant names of devices and tags when entering settings that identify a tag).

      If the script code does not fit into the **Lua script for rule** field, you can click to open a separate window for displaying the code.

   d. Configure the settings for registering an event when the rule is triggered (event title, description and score, and settings for saving traffic).

5. Click **Save**.

Editing Process Control rule settings

To edit Process Control rule settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Rules** tab, select the rule that you want to edit.

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

4. Click **Edit**.

5. Change the settings as necessary. You can edit the settings by using the same operations that were available when creating Process Control rules with conditions or Lua scripts.

Creating, viewing and editing a global Lua script

Variables and functions defined in a global Lua script can be used in rules with Lua scripts.

Users with the Administrator, Security Officer, or ICS Officer role can create and modify a global Lua script for Process Control rules. Users with any role can view the contents of a global Lua script.

To create or edit a global Lua script:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Rules** tab, open the global Lua script editing window by clicking **Global Lua script**.

4. Enter the code of the script in the Lua language.

5. Click **Save**.

Deleting Process Control rules

To delete Process Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with the Administrator, Security Officer, or ICS Officer role.

2. Select the **Process control** section.

3. On the **Rules** tab, select the rules that you want to delete.

4. Click **Delete**. If the button is not displayed in the toolbar, click the ⋮ button and select the desired item in the menu that opens.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm deletion of the rules.

Configuring Interaction Control

Kaspersky Industrial CyberSecurity for Networks can monitor the network interactions of devices in the industrial network. *Interaction Control rules* are used to define authorized and unauthorized network interactions. All detected network interactions that do not satisfy the active Interaction Control rules are considered to be unauthorized. The application registers the corresponding events when unauthorized interactions are detected.

An Interaction Control rule can be applied by one of the following technologies:

- Network Integrity Control – the rule describes network interaction between devices using a specific set of protocols and connection settings.

- Command Control – the rule describes the monitored system commands during communications between devices over one of the supported protocols for Process Control.

An Interaction Control rule contains the following information about interactions/communications:

- Sides participating in network interactions.

- Allowed protocol or system commands.

Network interactions between devices are identified based on the MAC- and/or IP addresses of the devices. If additional address spaces were added to the application, you can configure Interaction Control rules for the addresses of relevant address spaces.

When analyzing network interactions for Network Integrity Control, the application also checks the IP addresses in these interactions to see if they belong to known subnets. IP addresses are verified for all IPv4 interactions. The application checks each interaction against Network Integrity Control rules (and registers the corresponding event if necessary), only if this interaction must be controlled according to the table below.

Subnets of IP addresses whose interactions are controlled

Source subnet	Destination subnet				
	Private, IT	Private, OT	Private, DMZ	Public	Link-local
Private, IT	no	yes	no	no	yes
Private, OT	yes	yes	yes	yes	yes
Private, DMZ	no	yes	no	no	yes
Public	no	yes	no	no	yes
Link-local	yes	yes	yes	yes	no

Example
When controlling interactions based on Network Integrity Control technology, the application checks all interactions in which the sources or destinations of network packets have IP addresses from **Private, OT** subnets. The application does not check interactions in which the destinations of network packets have IP addresses from **Private, DMZ** subnets while the network packet sources have IP addresses from **Private, IT** subnets.

Command Control technology is applied regardless of the specific subnet of the IP addresses of the sources and destinations of network packets containing system commands.

Interaction Control rules can be enabled or disabled.

By default, a rule is enabled after it is created and is applied to allow the described communications. The application does not register events when it detects interactions that are described in enabled rules.

Disabled rules are intended for describing unwanted network interactions. In learning mode for Interaction Control technologies, disabled rules prevent automatic creation of new enabled rules that describe the same network interactions. In monitoring mode, disabled rules are not taken into account.

The application processes Interaction Control rules based on Network Integrity Control and Command Control technologies if the use of these technologies is enabled. You can also configure the learning mode for these technologies.

The following methods are provided for creating a list of Interaction Control rules:

- Automatic generation of rules in learning mode
- Automatic generation of rules when importing configurations from external projects
- Fine-tuning Interaction Control for individual devices
- Manual creation of rules

You can configure Interaction Control rules in the **Allow rules** section of the Kaspersky Industrial CyberSecurity for Networks web interface. This section contains a table with Interaction Control rules based on Network Integrity Control and Command Control technologies. This rules table may also contain allow rules created for events.

Events registered based on Network Integrity Control and Command Control technologies are categorized as system events.

You can view Interaction Control events in the table of registered events. Events registered based on Network Integrity Control technology have *High* severity. Events registered based on Command Control technology are assigned a severity that depends on the severity level defined for the detected system command.

Learning mode for Interaction Control technologies

To reduce the number of same-type actions and to automate the process of creating and configuring rules, the application uses machine learning methods and baseline models. The application analyzes various patterns in the network activity of devices that are detected during traffic processing and generates ready-to-use Interaction Control rules. Machine learning methods are used when learning mode is enabled.

In Interaction Control learning mode, the application does the following:

- If use of Network Integrity Control technology is enabled, the application generates rules based on this technology. Rules are generated for all IPv4 interactions that must be controlled according to the IP address subnet table for interaction control. When the application detects network interactions that match disabled rules, it registers events based on Network Integrity Control technology. The events are registered using the system event type that is assigned the code 4000002601.

- If the use of Command Control technology is enabled, the application generates rules based on this technology. When the application detects system commands that match disabled rules, it registers unauthorized system command detection events based on Command Control technology. The event is registered using the system event type that is assigned the code 4000002602.

When generating rules based on Interaction Control technologies, the application adds new rules obtained from its analysis of network interactions and system commands in industrial network traffic. For these rules, the **Source** value is set to **System**. If you manually change rule settings, **Source** will be set to **User**.

Network interactions detected during traffic analysis are checked for compliance with current Interaction Control rules. If a detected interaction does not match any rule, the application creates a new rule. In this case, an interaction detection event is not registered. When a new rule is created, the application enables it and adds values of settings based on the received data about the network interaction.

If the detected interaction only matches a disabled rule, the application registers an event based on the technology corresponding to this rule. In this case, a new rule is not created.

During the learning process, the application can optimize the list of Interaction Control rules. Optimization involves combining two or more specific rules into one general rule, or deleting specific rules if a general rule is available. Rules that satisfy the following conditions are optimized:

- The rules are enabled.

- **Source** is set to **System**.

- The rules are related to the same technology.

Rules are merged during optimization if the resulting general rule will correspond only to the detected network interactions and no others. For example, one Interaction Control rule was created after a system command was detected during an interaction between two devices. Then another system command was detected during interaction between the same devices. In this case, after optimization, only one general rule will remain. It will describe both system commands detected during network interaction between these devices.

While operating in learning mode, the application periodically optimizes rules for the corresponding Interaction Control technology. The frequency of optimization is once per minute. Optimization is performed if new interactions are detected in industrial network traffic. To keep the rules table up to date, you must update rules.

After learning mode is disabled, optimization is performed one more time.

> There may be a delay before the Interaction Control rules are optimized after learning mode is disabled. The length of the delay depends on the amount of data being received by the application, and may last up to three minutes. During this time, it is recommended to refrain from making any changes to rules that were generated during learning mode based on Network Integrity Control and Command Control technologies.

Interaction Control learning mode must be enabled for enough time to receive all the necessary information about network interactions. This amount of time depends on the number of devices in the industrial network and how frequently they operate and are serviced. We recommend that you enable learning mode for at least one hour. In large industrial networks, learning mode can be enabled for a period ranging from one to several days to accumulate the maximum amount of data.

Monitoring mode for Interaction Control technologies

In Interaction Control monitoring mode, the application does the following:

- If use of Network Integrity Control technology is enabled, the application checks devices' network interactions for compliance with the rules based on this technology. When the application detects network interactions for which there are no enabled rules, it registers unauthorized communication detection events based on Network Integrity Control technology. The events are registered using the system event type that is assigned the code 4000002601.

- If use of Command Control technology is enabled, the application checks devices' network interactions for compliance with the rules based on this technology. When the application detects system commands for which there are no enabled rules, it registers unauthorized system command detection events based on Command Control technology. The event is registered using the system event type that is assigned the code 4000002602.

Rules related to different technologies are applied independently of each other. Therefore, to allow use of a system command, the allow rules table must have rules created (automatically or manually) for this system command and for a network packet that transmits this command.

Automatic generation of Interaction Control rules in learning mode

In learning mode, Kaspersky Industrial CyberSecurity for Networks automatically generates Interaction Control rules. The application creates a new rule if the detected network interaction does not match any rule in the allow rules table.

When creating a rule, the application defines the values of parameters that are received from traffic pertaining to a detected network interaction.

If a Network Integrity Control rule is being created for an interaction in which the IP address of one of the sides of communication is in a subnet known to the application, the application might not add MAC addresses detected together with this IP address to the rule settings. Detected MAC addresses for IP addresses of a subnet are added if the **Ignore MAC addresses for NIC rules** toggle is switched off in the subnet settings.

In learning mode, the application can automatically create Interaction Control rules that allow transmission of system commands for Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes. These rules are needed for convenient joint use of applications within the integrated Kaspersky Industrial CyberSecurity solution. To automatically create rules prior to enabling learning mode, you must enable the PLC Project Integrity Check component on computers with Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes installed in this same industrial network. For detailed information on enabling this component, please refer to the Help System for Kaspersky Industrial CyberSecurity for Nodes / Kaspersky Industrial CyberSecurity for Linux Nodes.

Automatic generation of Interaction Control rules when importing configurations from external projects

Kaspersky Industrial CyberSecurity for Networks automatically generates Interaction Control rules when importing configurations from a project for IEC 61850 devices. The application creates new rules based on information about devices in the configuration being imported.

After loading the project, Kaspersky Industrial CyberSecurity for Networks checks whether data in the traffic exchanged between the devices conforms to the imported configuration. If Kaspersky Industrial CyberSecurity for Networks detects irregularities in the traffic, it logs events.

If the configuration being imported defines protocols and connection settings for communications between devices, the application creates a Network Integrity Control rule. When the application detects network interactions that match disabled rules, it registers events based on Network Integrity Control technology.

If the configuration being imported defines system commands used for communications between devices, the application creates a Command Control rule. When it detects system commands that match disabled rules, it logs detections of unauthorized system commands using Command Control.

For rules created when importing configurations from a project for IEC 61850 devices, **Source** is set to **System**. If you manually change rule settings, **Source** will be set to **User**.

Viewing Interaction Control rules in the table of allow rules

Interaction Control rules are displayed in the allow rules table in the **Allow rules** section of the application web interface. Interaction Control rules include the following types:

- NIC rules based on Network Integrity Control technology.
- CC rules based on Command Control technology.

The settings of Interaction Control rules are displayed in the following columns of the table:

- **Rule ID**

  Unique ID of the rule.

- **Status** (◐ icon)

  Current status of the rule (*Enabled* or *Disabled*).

- **Rule type**

  For Interaction Control rules, this indicates the technology of the rule (NIC or CC). The EVT type is indicated for rules that disable event registration.

- **Protocols/Commands**

  For rules related to Network Integrity Control technology (NIC type) or rules that disable event registration (EVT type), this is the set of utilized protocols. For rules related to Command Control technology (CC type), this is the protocol and system commands. The protocols that are determined by the application based on the contents of network packets are italicized.

- **Side 1**

  Device name/address information of one of the sides of network interaction. You can enable or disable the display of addresses and ports of address information by using the following settings: **MAC address**, **IP address**, and **Port number**. If additional address spaces were added to the application, you can enable or disable the display of names of address spaces by using the following settings:

  - **AS for MAC addresses** – address spaces containing the MAC addresses in the Interaction Control rule. This setting can contain the names of only those address spaces that have address space rules with **Data Link (L2)** selected as the OSI model layer.

  - **AS for IP addresses** – address spaces containing the IP addresses in the Interaction Control rule. This setting can contain the names of only those address spaces that have address space rules with **Network (L3)** selected as the OSI model layer.

- **Side 2**

  Device name/address information of the other side of network interaction. The display of address information can be configured the same way as the **Side 1** column.

- **Comment**

  Additional information about the rule.

- **Created**

  The date and time when the rule was created.

- **Changed**

  The date and time when the rule was last modified.

- **Rule in event**

  The name of the Process Control rule or Intrusion Detection rule that must be indicated in the event (for EVT rules).

- **Monitoring point**

  The name of the monitoring point that must be indicated in the event (for EVT rules).

- **Event type**

  ID and title of the event type (for EVT rules).

- **Source**

  Information about the origin of the rule.

When viewing the rules table, you can use the configuration, filter, search, and sorting functions.

Fine-tuning Interaction Control for individual devices

When Interaction Control technologies are running in monitoring mode, the application registers events whenever detected interactions between devices do not comply with the enabled Interaction Control rules. Such events are considered *deviations in the network behavior* of devices. You can use these events to fine-tune (retrain) Interaction Control applied to individual devices. The fine-tuning consists of automatically creating allow rules based on registered events using Network Integrity Control and Command Control technologies.

Allow rules for network behavior deviations are automatically created for events related to the selected devices if the *Resolved* status has not yet been assigned to these events. After automatically creating allow rules, the application assigns the *Resolved* status to these events.

You can view information about the number of unprocessed events that were registered while monitoring the network interactions of a device. The information is displayed in the device details area on the **Network behavior** tab. To view detailed information about the registered events, you can navigate to the table of events by using the **Learning quality** widget.

To fine-tune Interaction Control for individual devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to create allow rules based on registered events.

4. Right-click to open the context menu.

5. In the context menu, select one of the following options:

   - **Complete device learning** if one device is selected.
   - **Complete learning of devices** if multiple devices are selected.

   A window with a confirmation prompt opens.

6. If there are risks associated with the network behavior deviation events of the selected devices and you want to assign the *Accepted* status to all of these risks at the same time, select the **Assign the Accepted status for risks related to the events** check box.

7. In the prompt window, confirm the fine-tuning of Interaction Control for the selected devices.

Manually creating Interaction Control rules

This section contains instructions on manually creating interaction control rule.

Creating an interaction control rule with blank settings or settings from a template

To create an interaction control rule with blank settings or settings from a template:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, open the details area by clicking **Add rule**.

3. If you want to define the values of settings from a template, in the details area click **Use template**, select the necessary template in the opened window and click **Apply**.

4. In the details area, select the rule type corresponding to the relevant Interaction Control technology:

   - If you want to create a rule based on Network Integrity Control technology, click **NIC**.
   - If you want to create a rule based on Command Control technology, click **CC**.

5. In the **Protocol** field, specify the protocol for interaction between devices.

   When the **Protocol** field is selected, a window opens showing the table of supported protocols displayed as a protocol stack tree. You can manage how tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   If necessary, use the search field above the table to find relevant protocols.

   To specify the protocol:

   a. In the protocols table, select the protocol that you want to specify for the rule. To select the relevant protocol, click the button that is displayed in the left column of the protocols table.

      For a Network Integrity Control rule, you can select any protocol that is displayed in the table of supported protocols. For a Command Control rule, you can select only a protocol from among the supported protocols for process control.

   b. Click **OK**.

   If you select a protocol that can be identified by the application based on the contents of network packets, a notification about this appears below the **Protocol** field.

6. If Command Control technology is selected for the rule, specify the relevant system commands in the **Commands** field.

   When the **Commands** field is selected, a window opens with a list of system commands that are available for the selected protocol. To specify the commands:

   a. In the list of system commands, select the check boxes next to the commands that should be allowed. If all commands should be allowed, you can either select all check boxes or clear all check boxes for all commands.

   b. Click **OK**.

7. If required, enter additional information about the rule in the **Comment** field.

8. In the **Side 1** and **Side 2** settings groups, specify the editable address information for the participants (sides) of network interaction. Depending on the selected protocol (or set of protocols), address information may contain a MAC address, IP address, and/or port number. If additional address spaces were added to the application, you can specify the names of the address spaces for addresses.

To autofill the address information of a side of network interaction, you can select devices that are known to the application. To do so:

a. Open the device selection window by clicking **Specify device addresses**.

b. In the device selection window, select the check boxes next to the devices that you want to use.

The device selection window contains a table in which you can configure the layout and order of columns, and also filter, search, and sort similarly to the table of devices in the **Assets** section.

c. Click **OK** in the device selection window.

9. In the details area, click **Save**.

The application checks the current list of Interaction Control rules.

10. If the Interaction Control rules include an enabled rule in which all the settings match, you will see a warning about the presence of a matching rule. In this case, close the warning and change the settings of the created rule.

11. If the Interaction Control rules include an enabled rule with more general settings, you will see a warning about the presence of a general rule. If a general rule is present, a new specific rule will not be used in the application. The warning will contain a prompt to save the new specific rule. To create a new rule with defined settings, confirm your decision in the prompt window (for example, if you want to then remove the general rule).

The new rule will be added to the allow rules table.

12. If the Interaction Control rules include enabled rules with more specific settings, you will see a warning about the presence of more specific rules. After a general rule appears, the specific rules will not be used in the application. The warning will contain a prompt to remove the specific rules. To remove specific rules, confirm your decision in the prompt window.

> If the rules table contains disabled rules with more specific or matching settings, the application removes these rules from the list. The application does not show a prompt when removing these rules.

13. If there is no enabled rule allowing network interaction between devices for a new rule based on Command Control technology, you will be prompted to create the corresponding rule based on Network Integrity Control technology. In this case, you are advised to create an additional rule together with the current rule being created. To do so, confirm your decision in the prompt window and perform the necessary actions to create a new rule based on Network Integrity Control technology.

Creating an interaction control rule from an existing one

To create an interaction control rule from an existing one:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, select the rule that you want to use as the basis for creating a new rule.

3. Right-click to open the context menu.

4. In the context menu, select **Copy rule**.

   The details area in rule editing mode will appear in the right part of the web interface window. The settings of the new rule will take the values obtained from settings of the selected rule.

5. Change the settings as necessary. To do so, complete steps 4–9 described in the procedure for creating a rule with initially empty values of settings.

Creating a rule based on an event registered for Network Integrity Control or Command Control technology

To create an interaction control rule from an event registered by Network Integrity Control or Command Control.

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator 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 an Interaction Control rule.

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

4. In the details area, click **Create allow rule**.

   The **Allow rules** section opens in the browser window. The details area in rule editing mode will appear in the right part of the web interface window. The new rule's settings will take the values received from the saved information about the event.

5. If necessary, edit the settings of the new rule. To do so, complete steps 4–9 described in the procedure for creating a rule with initially empty values of settings. If you do not need to change the settings of the new rule, save the rule by clicking **Save**.

Editing Interaction Control rule settings

You can edit the settings of an enabled Interaction Control rule. You cannot edit disabled rules.

To edit the settings of an Interaction Control rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, select the relevant NIC or CC rule to edit its settings.

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

3. Click **Edit**.

4. Change the settings as necessary.

Enabling and disabling Interaction Control rules

Interaction Control rules can be assigned a status of *Enabled* or *Disabled*. Rules are enabled by default after they are created.

You can disable rules that should not be used when Interaction Control technologies are operating in monitoring mode.

To change the status of the Interaction Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, select the Interaction Control rules for which you want to change the status.

3. Enable or disable rules by clicking **Enable** or **Disable**. The buttons that are displayed depend on whether their corresponding operations are relevant for one or more of the selected rules.

   If all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1000, the application does not check the status of the rules. If this is the case, the details area displays both buttons for changing the state of rules.

Suspending and resuming monitoring of the network interactions of devices

By default, monitoring mode for Interaction Control technologies is applied to all devices in the industrial network. If necessary, you can temporarily suspend monitoring of network interactions for individual devices (for example, if the device is involved in ongoing maintenance and commissioning work). If network interaction monitoring is suspended for a device, the application does not register unauthorized interaction alert events or unauthorized system command alert events for this device.

After the device returns to normal operation, you can resume monitoring of network interactions for this device.

It is not recommended to suspend monitoring of network interactions for devices that perform network switching functions between industrial network segments (routing devices). If you suspend monitoring for such a routing device, this could negatively affect the application of Interaction Control rules for devices that communicate through this routing device on different industrial network segments.

You can view information about the device's network behavior in the device details area on the **Network behavior** tab. The current status of monitoring the device's network interactions is displayed in the **Network Interaction Control** widget. Information about the number of unprocessed events registered while monitoring the device's network interactions is displayed in the **Learning quality** widget. Some quantitative values in widgets allow you to navigate to the corresponding sections of the application web interface. For example, to view detailed information about the unprocessed events, you can navigate to the table of events from the **Learning quality** widget.

To suspend or resume monitoring of the network interactions of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices for which you want to suspend or resume monitoring of network interactions.

4. Right-click to open the context menu.

5. In the context menu, select the relevant option: **Network behavior** → **Suspend monitoring** or **Network behavior** → **Resume monitoring**.

   A window with a confirmation prompt opens.

6. In the prompt window, confirm whether you want to suspend or resume monitoring of network interactions.

Deleting Interaction Control rules

You can selectively delete one or multiple Interaction Control rules. Rules that are deleted are no longer applied for Interaction Control technologies, whether in monitoring mode or learning mode.

To delete Interaction Control rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Allow rules** section.

3. In the rules table, select the Interaction Control rules that you want to delete.

4. Click **Delete**.

   A window with a confirmation prompt opens. Depending on the state of the selected rules, the prompt will suggest the following options:

   - If all selected rules are enabled, the application prompts you to delete the selected rules, disable them, or cancel the operation. This condition is not checked if all rules that satisfy the current filter and search settings are selected and the number of selected rules is more than 1000.

   - If there are disabled rules among the selected rules or if all rules that satisfy the current filter and search settings are selected, and the number of selected rules is more than 1000, the application prompts you to delete the selected rules or cancel the operation.

5. In the prompt window, confirm deletion of the rules.

Configuring Intrusion Detection and Network Anomaly Detection

Kaspersky Industrial CyberSecurity for Networks can analyze incoming industrial network traffic for signs of intrusions, attacks, and various anomalies. For these purposes, you can use intrusion detection rules, intrusion detection methods based on built-in algorithms, and network anomaly detection rules. If rules or built-in algorithms are triggered during traffic analysis, the application uses the Intrusion Detection technology to register events.

Methods and rules can be configured when connected to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. Configurable sets of intrusion detection rules and network anomaly detection rules are displayed in the **Detection rules** section. The application allows you to enable or disable the use of detection technologies and methods in **Settings** → **Deployment**.

You can view Intrusion Detection and Network Anomaly Detection events in the table of registered events.

Managing Intrusion Detection rule sets

An *Intrusion Detection rule* describes a traffic anomaly that could be a sign of an attack in the industrial network. The rules contain the conditions that the Intrusion Detection system uses to analyze traffic.

Intrusion Detection rules are stored on the Server and sensors.

The application applies intrusion detection rules when using the rule-based intrusion detection method. You can enable and disable this method.

Intrusion detection rules are grouped into sets of rules based on some attributes. For example, rules can be grouped by their purpose and included in a set designed to detect certain types of intrusions. You can use the following types of rule sets:

- System rule sets. These rule sets are provided by Kaspersky and are intended for detecting signs of the most frequently encountered attacks or unwanted network activity. System rule sets are available immediately after the application is installed. You can update system sets of rules by installing updates.

- User-defined rule sets. These rule sets are loaded into the application separately by the user. To load them, you need to use files containing data structures that define Intrusion Detection rules. These files must be in the same folder and have the RULES extension. The names of user-defined rule sets must match the names of the files from which these rule sets were loaded.

The application supports the application of no more than 50,000 rules cumulatively in all loaded rule sets. The limit on the number of loaded rule sets is 100.

> Rules loaded from user-defined rule sets may contain traffic analysis conditions whereby the application will register an excessive number of events when these rules are triggered. In this case, keep in mind that logging too many events may affect the performance of the Intrusion Detection System.

Sets of Intrusion Detection rules can be either enabled or disabled. Rules from the enabled set are applied during traffic analysis if the rule-based Intrusion Detection method is enabled. If a rule set is disabled, the rules from this rule set are not applied.

When a rule set is loaded, the application verifies the rules in the rule set. If errors are detected in the verified rules, the application blocks these rules from being applied. If errors are detected in all rules of the rule set or the rule set does not contain any rules, the application disables this rule set.

For information about sets of rules and detected errors, please refer to the **Detection rules** → **Intrusion Detection** section.

When the conditions defined in a rule from an enabled rule set are detected in traffic, the application registers a rule-triggering event. Events are registered with system event types that are assigned the following codes:

- 4000003000 – for an event when a rule from a system rule set is triggered.
- 4000003001 – for an event when a rule from a user-defined rule set is triggered.

User-defined rule sets may contain rules that were received from other Intrusion Prevention and Detection systems. When processing these rules, the application does not perform their defined actions that would otherwise be applied to network packets (for example, the `drop` and `reject` actions). When Intrusion Detection rules are triggered in Kaspersky Industrial CyberSecurity for Networks, only event registration is performed.

The scores of Kaspersky Industrial CyberSecurity for Networks events correspond to the specific priorities in Intrusion Detection rules (see the table below).

Mapping rule priorities to event scores

Intrusion Detection rule priority	Kaspersky Industrial CyberSecurity for Networks event score values
4 or higher	2.5
3	4.5
2	6.5
1	9

Enabling and disabling sets of Intrusion Detection rules

Sets of Intrusion Detection rules can be assigned a status of *Enabled* or *Disabled*. If a set of rules is disabled, no rules in this set are used for Intrusion Detection.

Whenever you enable or disable selected rule sets on all computers that have application components installed (Server and sensors), the Intrusion Detection system is restarted. A restart is required to apply the changes.

Users with the Administrator or Security Officer role can change the states of Intrusion Detection rule sets.

To change the status of Intrusion Detection rule sets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. In the **Detection rules** → **Intrusion Detection** section, select the sets of rules whose status you want to change.
3. Right-click to open the context menu.

4. In the context menu, select one of the following options:

   - **Enable** if you want to enable all disabled sets of rules from among the selected rule sets.
   - **Disable** if you want to disable all enabled sets of rules from among the selected rule sets.
   - **Change the statuses of selected rule sets** if you want to invert the statuses of all selected rule sets. This option lets you quickly enable or disable selected sets of rules with different statuses on all computers that have application components installed, as the Intrusion Detection System is restarted on all computers only once to apply all the changes together.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Loading and replacing user-defined sets of Intrusion Detection rules

You can load sets of Intrusion Detection rules from files into the application. Files containing descriptions of Intrusion Detection rules must be in the same folder and have the rules extension before you can load them into the application. The names of the files must not contain the following characters: `\ / : * ? , " < > |`.

After loading Intrusion Detection rules from a file, the rules are saved in the application as a user-defined rule set. The name of a rule set matches the name of the file from which this rule set was loaded.

When sets of rules are loaded from files, the current user-defined rule sets are deleted from the table and replaced with the new ones. However, system sets of rules (whose **Source** column shows the **System** value) are not deleted from the table.

Users with the Administrator or Security Officer role can load user-defined sets of Intrusion Detection rules.

To load and replace user-defined sets of Intrusion Detection rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Detection rules** → **Intrusion Detection**.
3. Click **Replace all user-defined rules** in the toolbar to open the window for selecting the folder containing Intrusion Detection rule files.
4. When the prompt window appears, click **OK**.
5. In the standard window of the browser you are using, select the folder containing the necessary files and click the button for transferring files from this folder.

   The table containing sets of rules displays the new user-defined sets of rules. For these sets of rules, the **Source** column shows the **User** value. All sets of rules that have no detected errors will be enabled.

6. Check for errors in rules within the loaded sets of rules.

   Information about the detected errors is displayed in the **Rules** column. A status of *OK* is displayed if there are no errors. If the set of rules contains errors, you can view detailed information about them by clicking **Details**.

7. If necessary, change the statuses of the rule sets (including the rule sets that have a status of *Errors in some rules*).

Removing user-defined sets of Intrusion Detection rules

You can remove all user-defined sets of Intrusion Detection rules that were loaded into the application from files. You cannot selectively remove individual user-defined sets of rules. If you want to use only some of the existing rule sets in the application, you can copy files containing these rule sets into a separate folder and replace all user-defined rule sets with the rule sets from this folder.

Users with the Administrator or Security Officer role can delete user-defined sets of Intrusion Detection rules.

To delete user-defined sets of Intrusion Detection rules:

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

2. Select **Detection rules** → **Intrusion Detection**.

3. Start deletion of user-defined rule sets by clicking **Delete all user-defined rules** in the toolbar.

   A window with a confirmation prompt opens.

4. In the prompt window, click **OK**.

All user-defined sets of Intrusion Detection rules will be deleted from the table.

Using additional Intrusion Detection methods

You can apply the following additional methods for Intrusion Detection:

- Detection of signs of falsified addresses in ARP packets (ARP spoofing).

  If detection of signs of falsified addresses in ARP packets is enabled, Kaspersky Industrial CyberSecurity for Networks scans the indicated addresses in ARP packets and detects signs of low-level man-in-the-middle (MITM) attacks. This type of attack in networks that use the ARP protocol is characterized by the presence of falsified ARP messages in traffic.

  When the application detects signs of falsified addresses in ARP packets, the application registers the events based on Intrusion Detection technology. Events are registered with system event types that are assigned the following codes:

  - 4000004001 – for detection of multiple ARP replies that are not associated with ARP requests.
  - 4000004002 – for detection of multiple ARP requests from the same MAC address to different destinations.

- TCP Protocol Anomaly Detection

  If TCP protocol anomaly detection is enabled, Kaspersky Industrial CyberSecurity for Networks scans TCP segments of the data stream in supported application-level protocols.

When it detects packets containing overlapping TCP segments with varying contents, the application registers an event based on Intrusion Detection technology. The events are registered using the system event type that is assigned the code 4000002701.

- IP Protocol Anomaly Detection

  If IP protocol anomaly detection is enabled, Kaspersky Industrial CyberSecurity for Networks scans fragmented IP packets.

  When the application detects errors in the assembly of IP packets, it registers events for Intrusion Detection technology. Events are registered with system event types that are assigned the following codes:

  - 4000005100 for detection of a data conflict when assembling an IP packet (IP fragment overlapped).
  - 4000005101 for detection of an IP packet that exceeds the maximum permissible size (IP fragment overrun).
  - 4000005102 for detection of an IP packet whose initial fragment is smaller than expected (IP fragment too small).
  - 4000005103 for detection of mis-associated fragments of an IP packet.

- Brute-force Attack and Scan Detection

  If Brute-force Attack and Scan Detection is enabled, Kaspersky Industrial CyberSecurity for Networks analyzes network activity statistics to detect signs of brute-force attacks on account credentials, denial of service, scans, network service spoofing, and other anomalies.

  This method uses built-in rules. When rules are triggered, the application registers an event based on Intrusion Detection technology. The events are registered using the system event type that is assigned the code 4000003002.

You can enable and disable these methods. You can apply additional Intrusion Detection methods regardless of the availability and state of Intrusion Detection rules. Embedded algorithms are used for the additional scan methods.

Managing Network Anomaly Detection rules

Network Anomaly Detection rules help detect traffic anomalies that may be indistinguishable from normal device activity at the network level. To detect such anomalies, the application analyzes the protocol attributes received in registered network sessions. A Network Anomaly Detection rule is triggered if any attributes, their values and/or patterns described in the rule are found. When a rule is triggered, Kaspersky Industrial CyberSecurity for Networks registers an event.

Protocol attributes consist of various characteristics of traffic in network sessions. These attributes are saved in a separate database on the Kaspersky Industrial CyberSecurity for Networks Server. The database used to store the attributes of protocols provides high-speed processing of both incoming data and requests for their analysis. To ensure that rule-based analysis has minimal impact on the DBMS and on the overall performance of the application, attribute search queries are executed in SQL. You can generate the necessary SQL queries in the rules yourself or use rule templates with ready-made SQL queries.

Network Anomaly Detection rule-based analysis is supported for attributes of the following protocols:

- DCE/RPC
- DNS

- Kerberos
- LDAP

The application saves protocol attributes in the database when using the method for getting attributes of protocols. You can enable and disable this method. To use the method for getting attributes of protocols, the Network Session Detection method must also be enabled. Both of these methods must be enabled on all nodes with installed application components from which information is received.

A rule-based search for network anomalies is performed among the protocol attributes received in the database during specific time intervals. The duration of the time interval for each rule is defined by the **Search depth** parameter. The duration is counted from the moment of the end boundary of the interval. Depending on how the rule is started, the time of the end boundary of the interval can be defined as follows:

- When the rule is automatically started according to a configured run schedule, the end boundary of the time interval coincides with the time when the rule is started.
- When the rule is manually started, you can manually define the date and time of the end of the interval.

To quickly configure the settings of the created Network Anomaly Detection rules, you can use the built-in rule templates. These templates are provided by Kaspersky. A list of templates that are built into the application is available immediately after installing the application. You can update the list of built-in templates by installing updates.

If a built-in template is not selected when creating a rule, the rule settings must be configured entirely manually (including writing the SQL query to search for protocol attributes in the database). In this case, the **User-defined** template is displayed as the template used for the rule. This same template is displayed if you have selected a built-in template and then change the settings that ensure the operating logic according to the selected built-in template, specifically the SQL query text or the main event registration settings. If you change other settings of the rule (for example, the automatic scheduled start settings or the threshold values in the variables of the SQL query) and all template values in the rule are not unlocked, the link between the rule and the selected built-in template is preserved.

The maximum number of network anomaly detection rules is 200.

Network Anomaly Detection rules can be enabled or disabled. If a rule is disabled, the application does not start this rule according to the configured schedule, and also blocks the capability to manually start this rule.

You can manage Network Anomaly Detection rules under **Detection rules → Network Anomaly Detection**. If you need to use dictionary values (for example, lists of IP addresses) for variables in SQL queries, you can create dictionaries with the necessary data under **Settings → Dictionaries**.

When a Network Anomaly Detection rule is triggered, an event is registered using a system event type, which is assigned the code 4000003003.

Creating Network Anomaly Detection rule

You are advised to use the appropriate built-in templates for the Network Anomaly Detection rules that you create. The templates contain configured settings (including ready-made SQL queries) for detecting typical anomalies. In most cases, after selecting a built-in template, you may only need to perform minor fine-tuning of some values for the created rule. For example, fine-tuning of template values may only be required for SQL query variables to change threshold values or specify created dictionaries.

To create a Network Anomaly Detection rule:

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

2. In the **Detection rules** → **Network Anomaly Detection** section, open the details area by clicking **Add rule**.

3. In the **Template** drop-down list, select the required template for the created rule.

   The values of rule settings will be defined according to the selected template.

   > If you leave the **User-defined** template selected, you will need to configure the rule settings entirely manually (including writing the SQL query text to search for protocol attributes in the database).

4. Enter the rule name and description.

5. Use the **Search depth** parameter to specify the duration of the time interval for searching for network anomalies among the protocol attributes received in the database. You can specify the time interval in seconds, minutes, hours, or days.

6. To run the rule according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

   a. In the **Frequency** drop-down list, select how often to run the job: **Every second**, **Every minute**, **Hourly**, **Daily**, **Weekly**, **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise job start time.

7. If you need to change the time period after which Kaspersky Industrial CyberSecurity for Networks will re-register a rule triggering event, turn on the **Change the default value** toggle switch and specify the necessary event regeneration period.

8. In the **Main event registration settings** block, check the settings for registering an event when the rule is triggered, and configure the settings if necessary. The settings are locked and cannot be edited if a built-in template is selected for the rule. In this case, to change the values of these settings, you must first click the **Unlock all template values** button above the field containing the selected template.

   > After clicking the **Unlock all template values** button, the link between the created rule and the selected built-in template is broken. The **User-defined** template is specified instead of the previously selected template for the rule.

   In the **Main event registration settings** block, you can specify values for the following settings of the event that the application will register when the rule is triggered:

   - Event title and description.

     When you enter a title or description for an event, tooltips or selectable General variables automatically appear next to the cursor.

   - Event score value.

9. Click the **SQL-specific query** tab.

The contents of the tab depend on the template that was selected at step 3:

- If a built-in template was selected, the **SQL-specific query** tab contains the text of the SQL query loaded from this template. The variables specified in the SQL query are listed in the **Utilized variables** block.
- If the **User-defined** template was selected, the tab contains no data. In this case, manually generate the text of the SQL query (see step 12).

10. If the **SQL-specific query** tab contains the SQL query text, test how this query works with the database. To do so, click the **Perform** button.

    The **Verify completion of SQL query** window appears and shows a table containing the results of the SQL query verification. To control the display of the window, use the buttons in the upper-right corner.

11. If necessary, fine-tune the SQL query by changing the values of the variables used in it. The variables are displayed in the **Utilized variables** settings block. You can define the values of variables explicitly or by using previously added dictionaries. To substitute the value of a variable from the dictionary, click opposite the variable and select the correct directory.

    You can use directories for variables with the "date", "time", "IP", "port", "string", or "weekday" data types. Dictionaries are not supported for variables with the "int" data type.

12. In the **SQL-specific query** field, check the text of the SQL query and generate any necessary text. The text of the SQL query is locked and cannot be edited if a built-in template is selected for the rule. In this case, to change the text, you must first click the **Unlock all template values** button above the field containing the selected template.

    > After clicking the **Unlock all template values** button, the link between the created rule and the selected built-in template is broken. The **User-defined** template is specified instead of the previously selected template for the rule.

    After generating the text of the SQL query, perform steps 10–11 again.

13. Click **Save**.

Changing Network Anomaly Detection rule

You can fine-tune created Network Anomaly Detection rules by changing their settings. For example, you can change the threshold values in the SQL query variables or specify other dictionaries for them. If a rule is still linked to a selected built-in template (in other words, a **User-defined** template is not specified), you cannot change the event registration settings and the SQL query text is not available in this rule. If you want to use the rule with other event registration settings or with a different SQL query, you can disable the current rule and create a new rule with the necessary settings.

Users with the Administrator or Security Officer role can change the Network Anomaly Detection rules.

To change the settings of a network anomaly detection rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Under **Detection rules** → **Network Anomaly Detection**, select the rule that you want to edit.

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

3. Click **Edit**.

4. Enter the rule name and description.

5. Use the **Search depth** parameter to specify the duration of the time interval for searching for network anomalies among the protocol attributes received in the database. You can specify the time interval in seconds, minutes, hours, or days.

6. To run the rule according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

   a. In the **Frequency** drop-down list, select how often to run the job: **Every second**, **Every minute**, **Hourly**, **Daily**, **Weekly**, **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise job start time.

7. If you need to change the time period after which Kaspersky Industrial CyberSecurity for Networks will re-register a rule triggering event, turn on the **Change the default value** toggle switch and specify the necessary event regeneration period.

8. In the **Main event registration settings** block, check the settings for registering an event when the rule is triggered, and configure them if necessary. The settings are locked and cannot be edited if a built-in template is selected for the rule.

   If the settings can be edited, you can specify values for the following settings of the event that the application will register when the rule is triggered:

   - Event title and description.

     When you enter a title or description for an event, tooltips or selectable General variables automatically appear next to the cursor.

   - Event score value.

9. Click the **SQL-specific query** tab.

10. If necessary, test how the SQL query works with the database. To do so, click the **Perform** button.

    The **Verify completion of SQL query** window appears and shows a table containing the results of the SQL query verification. To control the display of the window, use the buttons in the upper-right corner.

11. If necessary, fine-tune the SQL query by changing the values of the variables used in it. The variables are displayed in the **Utilized variables** settings block. You can define the values of variables explicitly or by using previously added dictionaries. To substitute the value of a variable from the dictionary, click opposite the variable and select the correct directory.

    You can use directories for variables with the "date", "time", "IP", "port", "string", or "weekday" data types. Dictionaries are not supported for variables with the "int" data type.

12. In the **SQL-specific query** field, check the text of the SQL query and generate any necessary text. The text of the SQL query is locked and cannot be edited if a built-in template is selected for the rule.

    After generating the text of the SQL query, perform steps 10–11 again.

13. Click **Save**.

Generating SQL query texts for Network Anomaly Detection rules

You can manually generate the texts of SQL queries when creating or modifying Network Anomaly Detection rules. Queries are intended for searching, extracting, and analyzing the attributes of protocols received in registered network sessions. Protocol attributes are stored in a separate database on the Kaspersky Industrial CyberSecurity for Networks Server. To access this database, you need to generate queries in the Structured Query Language (SQL), which is supported by the ClickHouse DBMS. For information about the supported queries that are used to perform actions for data extraction and analysis, see ClickHouse Help.

You are advised to use one of the built-in rule templates to generate the SQL query text. You can select a template when creating a rule. You can select a template that is most similar in purpose to the task that you want to perform. After selecting a built-in template to generate other SQL query text, you need to click the **Unlock all template values** button.

When you enter SQL query strings in the window, lists of suitable functions, operators, and settings are automatically displayed. You can select the items that you need from these lists for quick insertion into the text of an SQL query.

Main functions and operators used in SQL queries for Network Anomaly Detection rules

Function	Description
`SELECT`	Contains an enumeration of the fields in the table containing information about network sessions. The listed fields are accessed based on an SQL query. The results of the selection from the query are used in part or in full to create a temporary table containing data for event enrollment. The fields of the temporary table are filled with values via an alias assignment mechanism. Aggregation functions (such as `sum`) and arithmetic operators (such as `+`) are supported. See the lists of table fields below.
`FROM`	Specifies the source of the data. The source can be specified as one of the following views, which are provided for queries to the table containing information about network sessions in the database used to store protocol attributes: • `{{sessions}}` to extract data while filtering based on a certain time interval. • `{{sessions_symmetric}}` is an extended variant of the `{{sessions}}` view, which adds symmetric network sessions (with the opposite direction of Source–Destination).
`WHERE`	Contains conditions for filtering data received from the source. A filter expression can contain comparison operations, logical operators, and the special function `PARAM_EQ`. The `PARAM_EQ` function lets you compare a value from the table with a variable defined in a rule. If a dictionary is selected for substituting variable values, the `PARAM_EQ` function must be specified in the SQL query. The general syntax for using the `PARAM_EQ` function is as follows: `PARAM_EQ(column_value, {{param_name:param_type}})` where: • `column_value` is the field or expression to be compared. • `{{param_name:param_type}}` refers to the variable and its type as defined in the rule for the SQL query.
`GROUP BY`	Switches the query to aggregation mode and specifies the list of fields or aliases by which you need to group the returned data.
`HAVING`	Contains conditions for filtering the results obtained using the `GROUP BY` operator.

Function	Description
`ORDER BY`	Contains a list for sorting the returned data. For list items, you can specify modifiers that determine the sorting direction: • `DESC` sorts in descending order. • `ASC` sorts in ascending order.

Fields of the table containing information about network sessions

In the database for storing the attributes of protocols, the table containing information about network sessions contains rows with data blocks (chunks) that were received during 15-second intervals. Each registered network session is presented in the table as separate data blocks, and calls in SQL queries must be made within these data blocks.

The table containing information about network sessions contains the following fields that can be called in SQL queries:

- `session_id`, type `UInt64`: unique identifier of the network session
- `chunk_start_time`, type `DateTime64(6, 'UTC')`: start time of the data block (chunk) related to the network session, with microsecond precision
- `partition_id`, type `UInt64`: ID of the partition in the data block (chunk)
- `start_time`, type `DateTime64(6, 'UTC')`: time of the first packet in the data block (chunk), with microsecond precision
- `end_time`, type `DateTime64(6, 'UTC')`: time of the last packet in the data block (chunk), with microsecond precision
- `sip`, type `IPv4`: source IP address (Side 1)
- `dip`, type `IPv4`: destination IP address (Side 2)
- `sport`, type `UInt16`: source port (Side 1)
- `dport`, type `UInt16`: destination port (Side 2)
- `smac`, type `FixedString(17)`: source MAC address (Side 1) in XX:XX:XX:XX:XX:XX format
- `dmac`, type `FixedString(17)`: destination MAC address (Side 2) in XX:XX:XX:XX:XX:XX format
- `smac_as_id`, type `UInt64`: source MAC address (Side 1) converted to a 64-bit integer
- `dmac_as_id`, type `UInt64`: destination MAC address (Side 2) converted to a 64-bit integer
- `sip_as_id`, type `UInt64`: source IP address (Side 1) converted to a 64-bit integer
- `dip_as_id`, type `UInt64`: destination IP address (Side 2) converted to a 64-bit integer
- `vlanid`, type `UInt16`: VLAN ID
- `ether_type`, type `UInt16`: type of Ethernet frame (for example: 2048 for IPv4)

- `ipv4_type`, type `UInt8`: IPv4 type (8-bit value)
- `protocol`, type `LowCardinality(String)`: name of the application layer protocol in the table (for example: `GenericDceRpc`, `Ssh`)
- `transport_protocol`, type `LowCardinality(String)`: name of the transport layer protocol in the table (for example: `Tcp`, `Udp`)
- `bytes_sent_delta`, type `UInt64`: amount of data sent during the period of the data block (chunk)
- `packets_sent_delta`, type `UInt64`: number of packets sent during the period of the data block (chunk)
- `bytes_received_delta`, type `UInt64`: amount of data received during the period of the data block (chunk)
- `packets_received_delta`, type `UInt64`: number of packets received during the period of the data block (chunk)
- `dpi_dns`, type `Array(Map(String, String))`: structured data on network events in traffic over the DNS protocol
- `dpi_dns_raw`, type `Array(String)`: JSON-formatted data on network events in traffic over the DNS protocol
- `dpi_krb`, type `Array(Map(String, String))`: structured data on traffic over the Kerberos protocol
- `dpi_krb_raw`, type `Array(String)`: JSON-formatted data on traffic over the Kerberos protocol
- `dpi_dcerpc`, type `Array(Map(String, String))`: structured data on traffic over the DCE/RPC protocol
- `dpi_dcerpc_raw`, type `Array(String)`: JSON-formatted data on traffic over the DCE/RPC protocol
- `dpi_ldap`, type `Array(Map(String, String))`: structured data on traffic over the LDAP protocol
- `dpi_ldap_raw`, type `Array(String)`: JSON-formatted data on traffic over the LDAP protocol
- `total_attributes`, type `UInt32 MATERIALIZED`: total number of attributes in the `dpi_dns_raw`, `dpi_krb_raw`, `dpi_dcerpc_raw`, and `dpi_ldap_raw` fields
- `dpi_attributes_raw`, type `Array(String) MATERIALIZED`: combined array of JSON-formatted data on attributes

Fields of the table containing data for event enrollment

The table containing data for event enrollment may contain the following fields, which are filled with values via the alias assignment mechanism in an SQL query:

- Required fields:
  - `aggregation_id`, type `String`: unique aggregation identifier that identifies the event
  - `session_ids`, type `Array(UInt64)`: array of network session IDs associated with the event

- `timestamp`, type `DateTime64(6, 'UTC')`: date and time of the first occurrence of the event
- `protocol`, type `String`: name of the protocol in the table containing information about network sessions (for example: `Ssh`)

- Fields for storing address information and other network interaction data in events (optional fields that can be completed in an SQL query):
  - `sip`, type `IPv4`: source IP address
  - `dip`, type `IPv4`: destination IP address
  - `sport`, type `UInt16`: source port
  - `dport`, type `UInt16`: destination port
  - `smac`, type `FixedString(17)`: source MAC address in XX:XX:XX:XX:XX:XX format
  - `dmac`, type `FixedString(17)`: destination MAC address in XX:XX:XX:XX:XX:XX format
  - `smac_as_id`, type `UInt64`: address space identifier for the source MAC address
  - `dmac_as_id`, type `UInt64`: address space identifier for the destination MAC address
  - `sip_as_id`, type `UInt64`: address space identifier for the source IP address
  - `dip_as_id`, type `UInt64`: address space identifier for the destination IP address
  - `vlanid`, type `UInt16`: VLAN ID
  - `ether_type`, type `UInt16`: type of Ethernet frame
  - `ipv4_type`, type `UInt8`: IPv4 type
- Arbitrarily named fields for specifying their values in events using the variable `$extra.<paramName>`.

Protocol names in the table containing information about network sessions

Path in the protocol stack tree	Protocol name in the table
Ethernet I	EthernetI
Ethernet I \ LLC \ Cisco Discovery Protocol (CDP)	Cdp
Ethernet I \ LLC \ Emerson Ovation: interactions over LLC	Emerson_Ovation_OverLlc
Ethernet I \ LLC \ Foxboro FCP280/FCP270: device interaction	`FoxboroHps`
Ethernet I \ LLC \ HiDiscovery	`HiDiscovery`
Ethernet I \ LLC \ IS-IS over Ethernet I	`IsIsOverEthernetI`
Ethernet I \ LLC \ ISO 8073 \ Siemens S7comm	`SiemensIndustrialEthernet`
Ethernet I \ LLC \ VNIIA	`Vniia`
Ethernet II	`EthernetII`

Ethernet II \ ARP	`ARP`
Ethernet II \ IEC 61850: GOOSE	`IEC61850_GOOSE`
Ethernet II \ IEC 61850: Sampled Values	`SAMPLED_VALUES`
Ethernet II \ IP	`IPv4`
Ethernet II \ IP \ 3PC	`ip34`
Ethernet II \ IP \ Active Networks	`ip107`
Ethernet II \ IP \ ARIS	`ip104`
Ethernet II \ IP \ AX.25	`ip93`
Ethernet II \ IP \ BBN RCC Monitoring	`ip10`
Ethernet II \ IP \ BNA	`ip49`
Ethernet II \ IP \ BR-SAT-MON	`ip76`
Ethernet II \ IP \ CBT	`ip7`
Ethernet II \ IP \ CFTP	`ip62`
Ethernet II \ IP \ CHAOS	`ip16`
Ethernet II \ IP \ Compaq-Peer	`ip110`
Ethernet II \ IP \ CPHB	`ip73`
Ethernet II \ IP \ CPNX	`ip72`
Ethernet II \ IP \ CRTP	`ip126`
Ethernet II \ IP \ CRUDP	`ip127`
Ethernet II \ IP \ DCCP	`ip33`
Ethernet II \ IP \ DCN-MEAS	`ip19`
Ethernet II \ IP \ DDP	`ip37`
Ethernet II \ IP \ DDX	`ip116`
Ethernet II \ IP \ DGP	`ip86`
Ethernet II \ IP \ DSR	`ip48`
Ethernet II \ IP \ EGP	`ip8`
Ethernet II \ IP \ EIGRP	`EIGRP`
Ethernet II \ IP \ EMCON	`ip14`
Ethernet II \ IP \ ETHERIP	`ip97`
Ethernet II \ IP \ FCIP	`ip133`
Ethernet II \ IP \ FIRE	`ip125`
Ethernet II \ IP \ GGP	`ip3`
Ethernet II \ IP \ GMTP	`ip100`
Ethernet II \ IP \ GRE	`GRE`
Ethernet II \ IP \ HMP	`ip20`
Ethernet II \ IP \ IATP	`ip117`
Ethernet II \ IP \ ICMP	`Icmp`
Ethernet II \ IP \ IDPR	`ip35`
Ethernet II \ IP \ IDPR-CMTP	`ip38`
Ethernet II \ IP \ IDRP	`ip45`
Ethernet II \ IP \ IFMP	`ip101`

Ethernet II \ IP \ IGMP	`IGMP`
Ethernet II \ IP \ IGP	`ip9`
Ethernet II \ IP \ I-NLSP	`ip52`
Ethernet II \ IP \ Internet Link	`ip40`
Ethernet II \ IP \ IPComp	`ip108`
Ethernet II \ IP \ IPCV	`ip71`
Ethernet II \ IP \ IPIP	`ip94`
Ethernet II \ IP \ IPLT	`ip129`
Ethernet II \ IP \ IPPC	`ip67`
Ethernet II \ IP \ IPv4 Encapsulated	`ip4`
Ethernet II \ IP \ IPv6 Encapsulated	`IPv6encapsulated`
Ethernet II \ IP \ IPX-in-IP	`ip111`
Ethernet II \ IP \ IRTP	`ip28`
Ethernet II \ IP \ IS-IS over IPv4	`IsIsOverIp`
Ethernet II \ IP \ ISO-IP	`ip80`
Ethernet II \ IP \ ISO-TP4	`ip29`
Ethernet II \ IP \ Kryptolan	`ip65`
Ethernet II \ IP \ L2TP	`ip115`
Ethernet II \ IP \ LARP	`ip91`
Ethernet II \ IP \ MANET	`ip138`
Ethernet II \ IP \ MERIT-INP	`ip32`
Ethernet II \ IP \ MFE-NSP	`ip31`
Ethernet II \ IP \ MICP	`ip95`
Ethernet II \ IP \ MOBILE	`ip55`
Ethernet II \ IP \ MPLS-in-IP	`ip137`
Ethernet II \ IP \ MTP	`ip92`
Ethernet II \ IP \ MUX	`ip18`
Ethernet II \ IP \ NARP	`ip54`
Ethernet II \ IP \ NETBLT	`ip30`
Ethernet II \ IP \ NSFNET-IGP	`ip85`
Ethernet II \ IP \ NVP-II	`ip11`
Ethernet II \ IP \ Open Shortest Path First (OSPF)	`Ospf`
Ethernet II \ IP \ Performance Transparency Protocol	`ip123`
Ethernet II \ IP \ PGM	`ip113`
Ethernet II \ IP \ PIM	`PIM`
Ethernet II \ IP \ PIPE	`ip131`
Ethernet II \ IP \ PNNI	`ip102`
Ethernet II \ IP \ PRM	`ip21`
Ethernet II \ IP \ PUP	`ip12`
Ethernet II \ IP \ PVP	`ip75`
Ethernet II \ IP \ QNX	`ip106`

Ethernet II \ IP \ Reliable Data Protocol	`RDP`
Ethernet II \ IP \ ROHC	`ip142`
Ethernet II \ IP \ RSVP	`ip46`
Ethernet II \ IP \ RSVP-E2E-IGNORE	`ip134`
Ethernet II \ IP \ RVD	`ip66`
Ethernet II \ IP \ SAT-EXPAK	`ip64`
Ethernet II \ IP \ SAT-MON	`ip69`
Ethernet II \ IP \ SCC-SP	`ip96`
Ethernet II \ IP \ SCPS	`ip105`
Ethernet II \ IP \ SCTP	`SCTP`
Ethernet II \ IP \ SDRP	`ip42`
Ethernet II \ IP \ SECURE-VMTP	`ip82`
Ethernet II \ IP \ SMP	`ip121`
Ethernet II \ IP \ SNP	`ip109`
Ethernet II \ IP \ Sprite-RPC	`ip90`
Ethernet II \ IP \ SPS	`ip130`
Ethernet II \ IP \ SRP	`ip119`
Ethernet II \ IP \ SSCOPMCE	`ip128`
Ethernet II \ IP \ STP	`STP`
Ethernet II \ IP \ SUN-ND	`ip77`
Ethernet II \ IP \ TCF	`ip87`
Ethernet II \ IP \ TCP	`Tcp`
Ethernet II \ IP \ TCP \ ABB SPA-Bus	`ABB_SpaBus`
Ethernet II \ IP \ TCP \ AeroAdmin over TCP	`AeroAdmin`
Ethernet II \ IP \ TCP \ AFP	`SrvTcp_AFP`
Ethernet II \ IP \ TCP \ Allen-Bradley EtherNet/IP	`AB_EtherNet_IP`
Ethernet II \ IP \ TCP \ Ammyy Admin over TCP	`AmmyyAdmin`
Ethernet II \ IP \ TCP \ AnyDesk over TCP	`AnyDesk`
Ethernet II \ IP \ TCP \ ARMS control protocol	`AsrkScada`
Ethernet II \ IP \ TCP \ BECKHOFF ADS/AMS	`Beckhoff`
Ethernet II \ IP \ TCP \ Bitcoin over TCP	`Bitcoin_OverTcp`
Ethernet II \ IP \ TCP \ BitTorrent over TCP	`BittorrentOverTcp`
Ethernet II \ IP \ TCP \ CIMPLICITY-Historian over TCP	`CIMPLICITYHistorian`
Ethernet II \ IP \ TCP \ CIMPLICITY-HMI/SCADA over TCP	`CIMPLICITYNetwork_OverTcp`
Ethernet II \ IP \ TCP \ CODESYS V2	`CodesysV2`
Ethernet II \ IP \ TCP \ CODESYS V3 Gateway	`CodesysGatewayV3Tcp`
Ethernet II \ IP \ TCP \ COS	`Cos`
Ethernet II \ IP \ TCP \ Dameware® MRC	`SrvTcp_DameWare_Mini_Remote_Control`
Ethernet II \ IP \ TCP \ DCE/RPC	`GenericDceRpc`
Ethernet II \ IP \ TCP \ DICOM® over TCP	`DICOM_over_TCP`
Ethernet II \ IP \ TCP \ DLMS/COSEM	`DlmsCosem`

Ethernet II \ IP \ TCP \ DMS for ABB AC 700F	`ABB_AC700F_DMS`
Ethernet II \ IP \ TCP \ DNP3	`Dnp3`
Ethernet II \ IP \ TCP \ DNS	`SrvTcp_DNS`
Ethernet II \ IP \ TCP \ DNS/LLMNR over TCP	`DnsLlmnr_OverTcp`
Ethernet II \ IP \ TCP \ Dogecoin over TCP	`Dogecoin`
Ethernet II \ IP \ TCP \ Emerson ControlWave Designer	`EmersonControlWaveDesigner`
Ethernet II \ IP \ TCP \ Emerson DeltaV - firmware update	`EmersonDeltaVFirmware`
Ethernet II \ IP \ TCP \ EtherNet/IP \ OMRON FINS	`OmronFinsEthernetIp`
Ethernet II \ IP \ TCP \ Ether-S-IO over TCP	`Esio_OverTcp`
Ethernet II \ IP \ TCP \ Finger	`SrvTcp_FINGER_PROTOCOL`
Ethernet II \ IP \ TCP \ Flash Media Server	`SrvTcp_Flash_Media_Server`
Ethernet II \ IP \ TCP \ FTP	`Ftp`
Ethernet II \ IP \ TCP \ FTP Data	`SrvTcp_FTP_DATA`
Ethernet II \ IP \ TCP \ General Electric SRTP	`Srtp`
Ethernet II \ IP \ TCP \ HL7® v2 over TCP	`HL7_ver2_over_TCP`
Ethernet II \ IP \ TCP \ HL7 v3 over TCP	`HL7_ver3_over_TCP`
Ethernet II \ IP \ TCP \ Honeywell ControlEDGE 900: device interaction	`HoneywellControlEdge`
Ethernet II \ IP \ TCP \ Honeywell Experion CDA	`HoneywellExperionCdaComm`
Ethernet II \ IP \ TCP \ Honeywell Experion EpicMo	`HoneywellExperionEpicMo`
Ethernet II \ IP \ TCP \ HTTP	`SrvTcp_HTTP`
Ethernet II \ IP \ TCP \ HTTP/2	`HTTP2`
Ethernet II \ IP \ TCP \ HTTPS	`SrvTcp_HTTPS`
Ethernet II \ IP \ TCP \ IBM® DB2®	`SrvTcp_IBM_DB2`
Ethernet II \ IP \ TCP \ Ident	`SrvTcp_Ident`
Ethernet II \ IP \ TCP \ IEC 60870-5-101	`IEC_60870_5_101`
Ethernet II \ IP \ TCP \ IEC 60870-5-104	`IEC_60870_5_104`
Ethernet II \ IP \ TCP \ IMAP	`SrvTcp_IMAP`
Ethernet II \ IP \ TCP \ IPU-FEU: device interaction	`Feu`
Ethernet II \ IP \ TCP \ IRC	`Irc`
Ethernet II \ IP \ TCP \ ISaGRAF IXL	`IsagrafIxl`
Ethernet II \ IP \ TCP \ ISaGRAF SNCP	`IsagrafSncp`
Ethernet II \ IP \ TCP \ ISO TSAP	`SrvTcp_Iso8072`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ IEC 61850: MMS	`IEC61850_MMS`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ MMS for ABB AC 800M	`ABB_AC800M_MMS`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ Siemens S7comm	`SiemensS7Comm`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ Siemens S7comm-plus	`SiemensS7CommPlus`
Ethernet II \ IP \ TCP \ ISO TSAP \ ISO 8073 \ TASE.2	`Tase2`
Ethernet II \ IP \ TCP \ Jabber® XMPP® over TCP	`Jabber`
Ethernet II \ IP \ TCP \ Kerberos over TCP	`SrvTcp_Kerberos`
Ethernet II \ IP \ TCP \ LDAP(S) over TCP	`SrvTcp_LDAP_S_`
Ethernet II \ IP \ TCP \ Litecoin over TCP	`Litecoin`

Ethernet II \ IP \ TCP \ Mitsubishi MELSEC System Q	`MitsubishiMelsecSystemQProtocol`
Ethernet II \ IP \ TCP \ MMS (ISO 9506-2)	`MmsBase`
Ethernet II \ IP \ TCP \ Modbus	`ModbusTcp`
Ethernet II \ IP \ TCP \ Modbus TCP for EKRA 200 series	`Ekra243Modbus`
Ethernet II \ IP \ TCP \ Moxa NPort: device configuration	`MoxaNportFirmware`
Ethernet II \ IP \ TCP \ Moxa NPort: device interaction	`MoxaNportIa5000aSystem`
Ethernet II \ IP \ TCP \ MQTT over TCP	`MQTT`
Ethernet II \ IP \ TCP \ MSNP	`SrvTcp_MSNP`
Ethernet II \ IP \ TCP \ MS SQL Server®	`SrvTcp_MS_SQL_Server`
Ethernet II \ IP \ TCP \ MySQL	`SrvTcp_MySQL`
Ethernet II \ IP \ TCP \ Napster	`SrvTcp_Napster`
Ethernet II \ IP \ TCP \ NetBIOS	`SrvTcp_NetBIOS`
Ethernet II \ IP \ TCP \ NFS	`SrvTcp_NFS`
Ethernet II \ IP \ TCP \ OMRON FINS	`OmronFinsTcp`
Ethernet II \ IP \ TCP \ ONVIF® over TCP	`ONVIF_over_TCP`
Ethernet II \ IP \ TCP \ OPC DA	`OpcDa`
Ethernet II \ IP \ TCP \ OPC UA Binary	`OpcUaBinary`
Ethernet II \ IP \ TCP \ Oracle DB	`SrvTcp_Oracle`
Ethernet II \ IP \ TCP \ POP3	`SrvTcp_POP3`
Ethernet II \ IP \ TCP \ PPTP	`SrvTcp_PPTP`
Ethernet II \ IP \ TCP \ Radmin application protocol over TCP	`Radmin_OverTcp`
Ethernet II \ IP \ TCP \ RDP	`SrvTcp_RDP`
Ethernet II \ IP \ TCP \ Relematika BDUBus	`BDUBus`
Ethernet II \ IP \ TCP \ Remote Utilities® over TCP	`RemoteUtilities`
Ethernet II \ IP \ TCP \ Rlogin	`SrvTcp_RLOGIN`
Ethernet II \ IP \ TCP \ RSH	`SrvTcp_RSH`
Ethernet II \ IP \ TCP \ RTSP over TCP	`RTSP_over_TCP`
Ethernet II \ IP \ TCP \ SAIA S-Bus over TCP	`Saia_OverTcp`
Ethernet II \ IP \ TCP \ Schneider Electric UMAS	`Umas`
Ethernet II \ IP \ TCP \ SFTP	`SrvTcp_SFTP`
Ethernet II \ IP \ TCP \ Siemens SICAM SCC: interaction with SICAM PAS	`NwChannel`
Ethernet II \ IP \ TCP \ SMB	`SrvTcp_SMB`
Ethernet II \ IP \ TCP \ SMB v2 over TCP	`Smb2_OverTcp`
Ethernet II \ IP \ TCP \ SMB v3 over TCP	`Smb3_OverTcp`
Ethernet II \ IP \ TCP \ SMTP	`SrvTcp_SMTP`
Ethernet II \ IP \ TCP \ SNMP	`SrvTcp_SNMP`
Ethernet II \ IP \ TCP \ SSH	`Ssh`
Ethernet II \ IP \ TCP \ SSL/TLS	`SslTls`
Ethernet II \ IP \ TCP \ SSL v2	`SslV2`
Ethernet II \ IP \ TCP \ SSL v3	`SslV3`
Ethernet II \ IP \ TCP \ SuiteLink over TCP	`SuiteLink`

Ethernet II \ IP \ TCP \ Syslog	`SrvTcp_Syslog`
Ethernet II \ IP \ TCP \ TeamViewer	`SrvTcp_TeamViewer`
Ethernet II \ IP \ TCP \ Telegram MTProto over TCP	`Telegram`
Ethernet II \ IP \ TCP \ Telnet	`Telnet`
Ethernet II \ IP \ TCP \ TFTP over TCP	`Tftp_OverTcp`
Ethernet II \ IP \ TCP \ TLS v1.0	`TlsV10`
Ethernet II \ IP \ TCP \ TLS v1.1	`TlsV11`
Ethernet II \ IP \ TCP \ TLS v1.2	`TlsV12`
Ethernet II \ IP \ TCP \ TLS v1.3	`TlsV13`
Ethernet II \ IP \ TCP \ TNS over TCP	`Tns_OverTcp`
Ethernet II \ IP \ TCP \ Tor® over TCP	`Tor_OverTcp`
Ethernet II \ IP \ TCP \ VNC	`SrvTcp_VNC`
Ethernet II \ IP \ TCP \ WebSocket	`WebSocket_OverTcp`
Ethernet II \ IP \ TCP \ WMI technology: device interaction	`Wmi`
Ethernet II \ IP \ TLSP	`ip56`
Ethernet II \ IP \ TP++	`ip39`
Ethernet II \ IP \ UDP	`UDP`
Ethernet II \ IP \ UDP \ BACnet	`Bacnet`
Ethernet II \ IP \ UDP \ BECKHOFF ADS/AMS	`BeckhoffUdp`
Ethernet II \ IP \ UDP \ BitTorrent over UDP	`BittorrentOverUdp`
Ethernet II \ IP \ UDP \ BSAP	`Bsap`
Ethernet II \ IP \ UDP \ CHINT MAS400: device interaction	`ChintMas400`
Ethernet II \ IP \ UDP \ CHINT MAS9600: device interaction	`ChintMas9600`
Ethernet II \ IP \ UDP \ CIMPLICITY-HMI/SCADA over UDP	`CIMPLICITYNetwork_OverUdp`
Ethernet II \ IP \ UDP \ CODESYS V3 Gateway	`CodesysGatewayV3Udp`
Ethernet II \ IP \ UDP \ Data Transfer Systems (DTS)	`Dts`
Ethernet II \ IP \ UDP \ DHCP	`Dhcp`
Ethernet II \ IP \ UDP \ DirectLOGIC: device interaction	`DirectLogicEcom`
Ethernet II \ IP \ UDP \ DNS	`SrvUdp_DNS`
Ethernet II \ IP \ UDP \ DNS/LLMNR over UDP	`DnsLlmnr_OverUdp`
Ethernet II \ IP \ UDP \ Dropbox LAN Sync over UDP	`DropBox_sync_OverUdp`
Ethernet II \ IP \ UDP \ Emerson DeltaV	`EmersonDeltaV`
Ethernet II \ IP \ UDP \ Emerson Ovation: multicast over UDP	`Emerson_Ovation_OverUdp_Mcast`
Ethernet II \ IP \ UDP \ Emerson Ovation: interactions over UDP	`Emerson_Ovation_OverUdp`
Ethernet II \ IP \ UDP \ Ether-S-IO over UDP	`Esio_OverUdp`
Ethernet II \ IP \ UDP \ General Electric EGD	`Egd`
Ethernet II \ IP \ UDP \ GLBP over UDP	`GLBP_OverUdp`
Ethernet II \ IP \ UDP \ Honeywell ControlEDGE 900: device detection	`HoneywellControlEdgeDiscovery`
Ethernet II \ IP \ UDP \ Honeywell Experion: device detection	`HoneywellExperionDiscovery`
Ethernet II \ IP \ UDP \ Honeywell Experion: getting device network configurations	`HoneywellExperionNameServer`
Ethernet II \ IP \ UDP \ HSRP over UDP	`HSRP_OverUdp`

Ethernet II \ IP \ UDP \ INA2000	`Ina2000`
Ethernet II \ IP \ UDP \ Kerberos over UDP	`SrvUdp_Kerberos`
Ethernet II \ IP \ UDP \ KNXnet/IP	`Knx`
Ethernet II \ IP \ UDP \ LDAP(S) over UDP	`SrvUdp_LDAP_S_`
Ethernet II \ IP \ UDP \ LDP	`SrvUdp_LDP`
Ethernet II \ IP \ UDP \ mDNS over UDP	`mDNS_OverUdp`
Ethernet II \ IP \ UDP \ MikroTik Neighbor Discovery Protocol (MNDP)	`Mndp`
Ethernet II \ IP \ UDP \ Moxa NPort: device detection	`MoxaNportDiscovery`
Ethernet II \ IP \ UDP \ MSNP	`SrvUdp_MSNP`
Ethernet II \ IP \ UDP \ NBNS over UDP	`NBNS_OverUdp`
Ethernet II \ IP \ UDP \ NetBIOS	`SrvUdp_NetBIOS`
Ethernet II \ IP \ UDP \ NFS	`SrvUdp_NFS`
Ethernet II \ IP \ UDP \ NTP	`SrvUdp_NTP`
Ethernet II \ IP \ UDP \ OMRON FINS	`OmronFins`
Ethernet II \ IP \ UDP \ PK4	`Pk4`
Ethernet II \ IP \ UDP \ PNU20	`Pnu20`
Ethernet II \ IP \ UDP \ QTP	`SrvUdp_QTP`
Ethernet II \ IP \ UDP \ RADIUS over UDP	`RadiusUdp`
Ethernet II \ IP \ UDP \ RDP	`SrvUdp_RDP`
Ethernet II \ IP \ UDP \ RIP	`RIP`
Ethernet II \ IP \ UDP \ SAIA S-Bus over UDP	`Saia_OverUdp`
Ethernet II \ IP \ UDP \ SCIYON default over UDP	`Sciyon`
Ethernet II \ IP \ UDP \ Siemens DIGSI 4	`SiemensDigsi4`
Ethernet II \ IP \ UDP \ SIP over UDP	`Sip`
Ethernet II \ IP \ UDP \ SMB over UDP	`Smb_OverUdp`
Ethernet II \ IP \ UDP \ SMB v2 over UDP	`Smb2_OverUdp`
Ethernet II \ IP \ UDP \ SMB v3 over UDP	`Smb3_OverUdp`
Ethernet II \ IP \ UDP \ SNMP	`SrvUdp_SNMP`
Ethernet II \ IP \ UDP \ SNMP v1 over UDP	`Snmpv1_OverUdp`
Ethernet II \ IP \ UDP \ SNMP v2 over UDP	`Snmpv2_OverUdp`
Ethernet II \ IP \ UDP \ SNMP v3 over UDP	`Snmpv3_OverUdp`
Ethernet II \ IP \ UDP \ SSDP	`SrvUdp_SSDP`
Ethernet II \ IP \ UDP \ Syslog over UDP	`Syslog_OverUdp`
Ethernet II \ IP \ UDP \ TeamViewer	`SrvUdp_TeamViewer`
Ethernet II \ IP \ UDP \ TFTP over UDP	`Tftp_OverUdp`
Ethernet II \ IP \ UDP \ TNS over UDP	`Tns_OverUdp`
Ethernet II \ IP \ UDP \ Tor over UDP	`Tor_OverUdp`
Ethernet II \ IP \ UDP \ Valmet DNA: device interaction	`Valmet`
Ethernet II \ IP \ UDP \ YARD	`Yard`
Ethernet II \ IP \ UDP \ Yokogawa Vnet/IP	`VnetIp`
Ethernet II \ IP \ UDPLite	`ip136`

Ethernet II \ IP \ UTI	`ip120`
Ethernet II \ IP \ VINES	`ip83`
Ethernet II \ IP \ VISA	`ip70`
Ethernet II \ IP \ VMTP	`ip81`
Ethernet II \ IP \ VRRP	`ip112`
Ethernet II \ IP \ VRRP over IPv4	`VRRP_OverIpv4`
Ethernet II \ IP \ WB-EXPAK	`ip79`
Ethernet II \ IP \ WB-MON	`ip78`
Ethernet II \ IP \ WESP	`ip141`
Ethernet II \ IP \ WSN	`ip74`
Ethernet II \ IP \ XNET	`ip15`
Ethernet II \ IP \ XNS-IDP	`ip22`
Ethernet II \ IP \ XTP	`ip36`
Ethernet II \ IPv6	`IPv6`
Ethernet II \ IPX	`IPX`
Ethernet II \ IS-IS over Ethernet II	`IsIsOverEthernetII`
Ethernet II \ Link Layer Discovery Protocol (LLDP)	`Lldp`
Ethernet II \ Loopback	`Loopback`
Ethernet II \ MiCOM C264	`MicomC264`
Ethernet II \ MPLS	`MPLS`
Ethernet II \ MPLS multicast	`MPLS_multi`
Ethernet II \ Precision Time Protocol	`PTP`
Ethernet II \ PROFINET IO	`ProfinetIo`
Ethernet II \ Prosoft-Systems: initial setup of devices	`ProsoftSystemsDeviceDiscovery`
Ethernet II \ PRP	`PRP`
Ethernet II \ RARP	`RARP`
Ethernet II \ RPC for PROFINET IO	`ProfinetRpc`

Using variables

You can add the following types of variables to the text of an SQL query:

- `string`: text string
- `date`: date in YYYY-MM-DD format
- `time`: time in hh:mm format
- `weekday`: number of the day of the week (1–7: 1 is Monday)
- `ip`: IPv4 address in XXX.XXX.XXX.XXX format

- `port`: port number (0–65535)
- `int`: 64-bit integer

To specify a variable and its type, use an entry in the format `{{param_name:param_type}}`. If the type of the variable is not specified (in an entry in the format `{{param_name}}`), the string type is used by default. The added variables are displayed below the SQL query text in the **Utilized variables** settings block. In this block, you can define the value of a variable or select a dictionary containing values for it.

When adding variables to an SQL query, please keep in mind that the maximum number of variables in an SQL query is 30.

Viewing the table of Network Anomaly Detection rules:

The network anomaly detection rules table is displayed in **Detection rules**, on the **Network Anomaly Detection** tab.

Users with the Administrator, Security Specialist, or Operator role can view the Network Anomaly Detection rules table.

On the **Network Anomaly Detection** tab, a **Delay of traffic receipt** counter is displayed under the toolbar. The counter contains the dynamically changing lag time of incoming traffic data received by the database used to store protocol attributes. If the application detects a critical lag time, the green icon is no longer displayed next to the counter. In this case, automatic runs of rules occurring during this period may lead to an incorrect result. Before returning the counter to its normal state, it is recommended to manually run the rules while taking into account the available range for analyzing protocol attributes.

The settings of rules are displayed in the following columns of the table:

- **Rule ID**

  Rule ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**

  Defined name of the rule.

- **Status**

  Current status of the rule (*Enabled* or *Disabled*).

- **Created**

  The date and time when the rule was created.

- **Changed**

  The date and time when the rule was last modified.

- **Template name**

  The name of the template associated with the rule. If the rule is not associated with a built-in template, the **User-defined** template is specified for the rule.

- **Search depth**.

  The duration of the time interval for searching for network anomalies among the protocol attributes.

- **Description**

  Rule description.

- **Schedule**

  Information about the schedule according to which the application automatically starts the rule.

- **Last run**

  Date and time when the rule was last started.

- **Status of last run**

  Resulting status of the rule when it was last run.

- **Number of events**.

  Number of events registered when the rule was run.

- **Event title**

  Header of the event registered when the rule is triggered.

- **Event score**

  Assessed score of the event that was registered when the rule was triggered. Events are scored on a scale from 0.0 to 10.0.

- **Event description**.

  Description of the event registered when the rule is triggered.

When viewing the Network Anomaly Detection rules table, you can use the configuration, filter, and sorting functions.

Enabling and disabling network anomaly detection rules

To enable or disable Network Anomaly Detection rules, you can change their status. Each rule can be assigned the *Enabled* or *Disabled* status. By default, the *Enabled* status is assigned to a rule after the rule is created.

If you assign the *Disabled* status to a rule, the application cancels the last run of the rule and assigns the **Canceled** status to this run. The last run of the rule is canceled if the run had a status of **New**, **Awaiting data**, **Pending**, or **Running** when the rule was disabled.

To change the status of Network Anomaly Detection rules:

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

2. Select **Detection rules**.

3. On the **Network Anomaly Detection** tab, select the rules for which you want to change the status.

4. Open the **Change status** drop-down list in the toolbar.

5. In the drop-down list, select the command to assign the required status.

Manually starting and stopping a Network Anomaly Detection rule

You can start and stop network anomaly detection rules manually. Stopping or starting a rule is available only for enabled rules.

A rule cannot run if it is in a status of **New**, **Pending**, **Awaiting data**, or **Running**.

To trigger the Network Anomaly Detection rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Detection rules**.
3. On the **Network Anomaly Detection** tab, select the rule you want to trigger.

   The details area appears in the right part of the web interface window.
4. Click **Run at interval**. The button is disabled if the rule cannot be triggered.

   The **Configure rule run** carrier appears on the right. The upper part of the panel displays information about the available range for analyzing protocol attributes. The range is limited to the earliest and latest arrival of traffic data in the database used to store protocol attributes.
5. Use the **Search depth** parameter to specify the duration of the time interval for searching for network anomalies among the protocol attributes. To manually run a rule, this value may be different from the value that was defined for the rule when it was created or when the settings were changed.
6. In the **Interval end** field, specify the date and time of the end of the time interval.
7. Click **Run**.

You can stop rules if they have one of the following statuses: **New**, **Pending**, **Awaiting data**, or **Running**.

To stop the execution of a network anomaly detection rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Detection rules**.
3. On the **Network Anomaly Detection** tab, select the rule that you want to stop.

   The details area appears in the right part of the web interface window.
4. Click **Stop** (this button is disabled if the rule cannot be stopped at this time).

Viewing general information about triggers for network anomaly detection rules

You can view an overview of how network anomaly detection rules are triggered when viewing the rule table. The table displays information about the most recent rule runs.

Users with the Administrator, Security Specialist, or Operator role can view general information about triggers for Network Anomaly Detection rules.

You can view general information about rule runs in the **Rule runs** settings block in the details area. General information about running network anomaly detection rules includes the following:

- Date and time when the rule was last started.
- Date and time of the next rule run.
- Status of last rule run

  The following statuses are available:

  - **Never run**: a new rule has been created and no run has been created for this rule.
  - **New**: a new run of the rule was created and an analysis of protocol attributes based on this rule has not yet been performed.
  - **Awaiting data**: Kaspersky Industrial CyberSecurity for Networks is waiting for traffic data to arrive in the database used to store protocol attributes (all data has not yet arrived by the end of the defined time interval for searching for network anomalies).
  - **Pending**: the rule is in the run queue.
  - **No data**: there is no traffic data in the time interval for searching for network anomalies based on the rule.
  - **Running**: the rule is running.
  - **Canceled**: the rule has been stopped.
  - **Completed**: the rule has been successfully completed.
  - **Error**: an error occurred while running the rule.
  - **Partially successful**: the rule was run with a partially successful result: traffic data was not received in full for the specified time interval.
- The number of times the rule runs.
- The duration of SQL query execution when the rule was last run.
- The time interval to search for network anomalies when the rule was last run.
- The number of events logged when the rule was last run.

Deleting Network Anomaly Detection rules

You can delete network anomaly detection rules. However, you cannot delete rules with a last run status of **New**, **Pending**, **Awaiting data**, or **Running**.

To delete the status of a Network Anomaly Detection rule:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Detection rules**.
3. On the **Network Anomaly Detection** tab, select the rules that you want to delete.
4. Click **Delete**.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the rules.

   Among the selected rules, you can delete only those rules for which the status of the last run differs from **New**, **Pending**, **Awaiting data**, and **Running**. If the selected rules contain any with a status of **New**, **Pending**, **Awaiting data**, or **Running**, a message about this will appear on the screen. To delete such rules, first stop the rules.

Managing dictionaries for Network Anomaly Detection rules

Kaspersky Industrial CyberSecurity for Networks implements storage of dictionary values for Network Anomaly Detection rules. You can use stored dictionary values in rules as the values of variables in SQL queries. *Dictionaries* are used to store dictionary values.

The application provides various types of dictionaries. Individual types of dictionaries are used to store IP addresses, port numbers, dates, and other data. Depending on the type of variable in the SQL query, you can select dictionaries of the corresponding type when creating or changing the settings of a Network Anomaly Detection rule.

You can manage dictionaries in the **Settings** → **Dictionaries** section. You can add up to 1000 dictionaries to the application. No more than 500 items can be added to each dictionary.

Users with the Administrator or Security Officer role can manage dictionaries.

Adding a dictionary

You can add dictionaries and use the elements saved in them as variable values in SQL queries for Network Anomaly Detection rules.

To add a dictionary:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Settings** → **Dictionaries**.
3. Open the details by clicking **Add dictionary**.
4. Enter the dictionary name and description.
5. Select the dictionary type and define its items.

You can select the following types of dictionaries:

- **Dates**, for storing dates. Corresponds to the "date" data type in the SQL query.
- **IP addresses**, for storing IP addresses. Corresponds to the "ip" data type in the SQL query.
- **Ports**, for storing port numbers. Corresponds to the "port" data type in the SQL query.
- **Text**, for storing string values. Corresponds to the "string" data type in the SQL query.
- **Time**, for storing time ranges. Corresponds to the "time" data type in the SQL query.
- **Days of the week**, for storing the days of the week. Corresponds to the "weekday" data type in the SQL query.

6. Click **Save**.

Viewing a dictionary table

The table of dictionaries for Network Anomaly Detection rules is displayed in the **Settings** → **Dictionaries** section of the application web interface.

Users with the Administrator, Security Specialist, or Operator role can view the dictionary table.

Information about dictionaries is displayed in the following columns of the table:

- **Dictionary ID**.
  Dictionary identifier assigned by Kaspersky Industrial CyberSecurity for Networks.
- **Name**
  Name used to represent the dictionary in the application.
- **Type**
  Dictionary type.
- **Number of items**.
  The number of items in the dictionary.
- **Created**
  Date and time when the dictionary was added to the application.
- **Changed**
  Date and time when the dictionary was last modified in the application.
- **Description**
  Description of the dictionary.

When viewing the dictionary table, you can use the configuration, filtering, and sorting functions.

Editing dictionary settings

When changing the settings of a dictionary, you can change its name, description and/or values of its items.

If the dictionary is already being used in a Network Anomaly Detection rule, the new values of dictionary elements will be applied only during the next run of the rule.

To change the dictionary settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Settings** → **Dictionaries**.
3. Select the dictionary you want to change.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. Change the settings as necessary. For a description of the settings, see the instructions for adding a dictionary.

Deleting dictionaries

You can delete dictionaries that are not used in the Network Anomaly Detection rules.

To delete a dictionary:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select **Settings** → **Dictionaries**.
3. Select the dictionary you want to delete.

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

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the dictionary.

Managing logs

This section contains information about managing logs of Kaspersky Industrial CyberSecurity for Networks.

Only users with the Administrator role can manage logs of Kaspersky Industrial CyberSecurity for Networks.

Managing the settings for storing logs in the Server database

You can change the settings for storing entries of logs in the Server database.

To change the settings for storing logs in the Server database:

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

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

   The details area will show the tabs for configuring the Server parameters.
5. On the **General** tab, configure the following settings in the **Events**, **Audit entries**, and **Application messages** sections:

   a. Use the **Max volume** setting to define the size limit for storing records. You can select the unit of measure for the value: **MB** or **GB**.

   When changing the value of this setting, please note the estimated maximum number of entries for the specified amount of space. You also need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

   b. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for entries, and specify the minimum number of days to store them.
6. Click **Save**.

Managing the settings for saving traffic in the Server database

The application can save traffic received at the moment when events are registered. Traffic is saved in the Server database when registering events for which traffic saving is enabled. The application can also save traffic in the Server database directly by requesting to load traffic using temporary traffic dump files.

The application saves traffic data in blocks. If a traffic block relates to several events (when events are registered in a short time interval), this traffic block is not duplicated in the database.

To change the settings for saving traffic in the Server database:

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

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

4. Click **Edit**.

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

5. On the **General** tab, go to **Traffic for events** and use the **Max volume** setting to define the size limit for storing traffic.

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

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

6. Click **Save**.

Managing the settings for saving traffic dump files

The application saves traffic received through the monitoring points as traffic dump files. These files are used by the application to analyze the incoming traffic. You can also use these files to perform the following actions in the application:

- Downloading traffic received by the node monitoring points
- Downloading traffic when working with the network interaction map
- Downloading network session traffic
- Downloading traffic for events (traffic dump files allow you to download traffic for events, even if traffic saving is disabled for the corresponding event types)

Traffic dump files are stored in the storages on the nodes where the application components are installed. On each node, both the internal storage of a node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used.

The application stores the traffic dump files temporarily. As traffic arrives, the application automatically deletes the oldest traffic dump files from the storages if the total volume of files approaches the limit set for the storage.

For each node, you can configure the settings for saving traffic to the internal storage. You can also connect the external storage of the node and configure the settings for saving traffic to the external storage.

To configure the settings for saving traffic dump files to the internal storage of the node:

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

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

3. Select the tile of the relevant node.

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

4. Click **Edit**.

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

5. If necessary, on the **General** tab, in the **Filtering stored traffic** section, enable filtering and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

   Filtering reduces the volume of the stored traffic by skipping the network packets that do not match the filter. However, when using filtering, keep in mind that the application may not receive all the data necessary for high-quality traffic analysis in the filtered traffic. Configure filtering so that all network packets that are required for traffic analysis according to the application functionality are saved in the traffic dump files.

6. Go to the **Traffic dump files** settings group and use the **Max volume** setting to define the size limit for storing traffic dump files.

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

   When changing the value of this setting, you need to keep in mind that the volume and rate of incoming traffic and the sum of all space limits cannot exceed the defined maximum storage limit for the node.

7. Click **Save**.

Enabling and disabling the user activity audit

You can enable and disable the application user activity audit.

User activity audit is enabled by default.

To enable or disable the user activity audit:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Audit**.
3. Use the **Audit** toggle button in the toolbar to enable or disable user activity audit.
4. Wait for the changes to be applied. The toggle switch is unavailable until it is finished moving to the other state.

Changing the logging level for processes

If application components are installed on nodes, these nodes have running processes that may save their operating data in logs. The table below describes the application processes whose operating data log storage you want to manage.

Application processes that are logged

Process	Server computer	Sensor computer	Description	Directory for storing logs
EntityManager	✓	✓	Process that controls the startup of other main processes of the application.	/var/log/kaspersky/kics4net/traces/EntityManager
Filter	✓	✓	Process that performs basic traffic analysis and receives telemetry from EPP applications.	/var/log/kaspersky/kics4net/traces/Filter
KisClient	✓	—	Process that downloads updates.	/var/log/kaspersky/kics4net/traces/KisClient

Process	Server computer	Sensor computer	Description	Directory for storing logs
NetworkDumper	✓	✓	Process that captures, filters, and saves traffic to disk.	/var/log/kaspersky/kics4net/traces/NetworkDumper
ProductServer	✓	—	Server to which all nodes of Kaspersky Industrial CyberSecurity for Networks are connected. The process provides the following functions: • Receive data from sensors. • Maintain a list of assets. • Provide access to the web server. • Write to the database. • Perform a detailed analysis of data received from the Filter process.	/var/log/kaspersky/kics4net/traces/ProductServer
Watchdog	✓	✓	Process that monitors the status of the main application processes and provides access to system counters and operating system statistics.	/var/log/kaspersky/kics4net/traces/Watchdog
WebServer	✓	—	Kaspersky Industrial CyberSecurity for Networks web interface	/var/log/kaspersky/kics4net-webserver/traces

For each process, you can assign one of the following logging levels:

- **Off**. Process data is not saved in the log. This level can be used to disable logging in an emergency situation, for example, if a large number of entries are saved to the log due to errors or circumstances associated with the environment.

- **Errors**. The log stores only data on errors that have occurred in process operations due to serious violations, most often resulting in data loss. Sometimes an entry of the **Errors** level indicates that some individual application modules are inoperable. As a rule, a log entry of this level is accompanied by a warning to the user in the form of an application message. This level can be used to temporarily switch from another logging level, for example, if the intensity of log entry generation prevents the detection of problems with the application.

  Example

  ```
  ERR [PDS] [PWS] ReadDbRuleFromCursor Custom value is empty for db protocol stack id: 227408
  ```

  This example shows an entry for a problem with one of the protocols in the protocol dictionary. The entry was assigned the **Errors** level because the problem affects all sessions with the specified protocol.

- **Warning** (default). The log stores data of the **Errors** level and data on minor internal violations that do not affect the performance of the application. Sometimes entries of this level contain informational messages that allow you to track the application loading process, for example.

  Example

  ```
  WRN [AMS] [AssetDiscovery] Ignore rule "TELNET Protocol" (id=200075). Wrong protocol stack table key.
  ```

  This example shows an entry about a problem with one of the thousands of detection rules that is using an incorrect protocol name. The entry was assigned the **Warning** level because the problem does not affect how the protocol is processed or the overall functionality of Kaspersky Industrial CyberSecurity for Networks.

- **Info**. The log stores data of the **Warning** level and important debug messages informing about the stages of application execution. This level is used to debug the application when too many log entries are generated at the **Debug** level.

Logging at this level may adversely affect the performance of Kaspersky Industrial CyberSecurity for Networks.

Example

```
INF [FILTER] [EKAIPC] Start: starting EkaIPCProvider...
```

This example shows an informational entry about the startup of an application module.

- **Debug**. The log stores data of the **Info** level and all data on process operations that may be required when debugging the application (for example, information about the steps for parsing packets of each network session). An entry of this level contains detailed information about the operation of the application. This level is used when analyzing a malfunction at the request of a Technical Support expert.

  Logging at this level creates an intensive load on the hard drive and significantly reduces the performance of Kaspersky Industrial CyberSecurity for Networks.
  Enabling this logging level can result in rapid deletion of previous entries according to the defined entry storage space limit. Investigation of the causes of error situations with this level is possible only for a short interval of time.

  Example

  ```
  DBG [SPDKP] [SiemensS7Comm Parser/0x576b87f0a888] Cyclic response detected: pduSequence = 0, sequence = 2,
  items size = 2
  DBG [NP3] Session 800000103cdb87f0a88b87f0a88e9200: reports sys command id #2405 on gpid: 164e8e5dec10c5
  DBG [SPDKP] [SiemensS7Comm Protocol/0x576bcabd3d58] Packet info: #127, 192.168.2.0:102 ==> 198.51.100.0:55671,
  Plc ==> Scada [82], time: 1779892008648825
  ```

  This example shows debug entries about handling the S7comm protocol. The entries contain the identifiers of the protocol handler and session, the IP addresses and ports of this session, the time of system command detection, and an indication of the scope of the traffic that needed to be handled.

The logging levels may need to be changed, for example, when contacting Technical Support.

Only users with the Administrator role can change logging levels.

Entries of the **Warning** level are logged for other less significant application processes. You cannot change the logging level for such processes. The logs of these processes are stored in the "traces" subdirectories of the corresponding local directories. For example, the logs of the rule-based network anomaly detection service are stored in the /var/log/kaspersky/kics4net-anomaly-hunter/traces directory.

To change logging levels for Kaspersky Industrial CyberSecurity for Networks processes:

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

2. Select **Settings** → **Logging**.

3. Change the logging levels as necessary:

   - To define the same logging level for all processes on all nodes, click the header of the column containing the name of the desired level.
   - To define the same logging level for all processes on one node, click a cell in the column containing the name of the desired level in the row containing the node name.
   - To define the log level for a process different from the logging levels defined for other processes, expand the list of processes of the relevant node in the **Nodes and processes** column and click a cell in the column containing the name of the necessary level in the row containing the process name.

4. Please wait for the changes to be applied (a progress indicator is displayed until the changes are fully applied).

Configuring operation with EPP applications

Kaspersky Industrial CyberSecurity for Networks can receive and process data received from Kaspersky applications that perform functions to protect workstations and servers. These applications are included in the Endpoint Protection Platform (EPP) and are installed to endpoint devices within the enterprise IT infrastructure.

Data transfer from EPP applications is performed by the *Endpoint Agent* software components. Depending on the version of the supported EPP application, the following software can perform the Endpoint Agent functions:

- Software modules built into the EPP application.
- Kaspersky Endpoint Agent application.

To connect to Kaspersky Endpoint Agent on devices running obsolete operating systems, such as Windows 7, Kaspersky Industrial CyberSecurity for Networks may rely on outdated and potentially vulnerable encryption protocols and algorithms. If there are no devices running obsolete operating systems on your network, or there is no need to connect to such devices, we recommend disabling obsolete and potentially vulnerable protocols and encryption algorithms in Kaspersky Industrial CyberSecurity for Networks. For more information, you can contact Technical Support.

The maximum number of computers from which data from EPP applications can be received and processed is 1000.

Data from computers with the Endpoint Agent software components is forwarded to Kaspersky Industrial CyberSecurity for Networks through *integration servers*. Integration server functions can be performed by any node that has a Kaspersky Industrial CyberSecurity for Networks component installed (Server or sensor). For integration with Endpoint Agent, add integration servers to the nodes that receive data from computers with Endpoint Agent.

An integration server can operate in TCP and UDP modes. Depending on the mode being used by the integration server on the node, Kaspersky Industrial CyberSecurity for Networks implements one of the following services for integration with EPP applications:

- kics4net-epp-proxy if TCP mode is enabled for the integration server.
- kics4net-telemetry-proxy if UDP mode is enabled for the integration server.

On each integration server, you can use TCP and UDP modes either separately or simultaneously. The installation packages for the services are included in the distribution kit of Kaspersky Industrial CyberSecurity for Networks.

In TCP mode, the integration server receives data from EPP applications and acknowledges the receipt of this data. This mode lets you perform various actions on devices hosting Endpoint Agent. In UDP mode, data from EPP applications is sent without confirmation of receipt via the UDP protocol. Due to the unidirectional data transmission over UDP, you can use UDP mode in cases where computers running Endpoint Agent transmit data to the integration server via data diode. However, the functional capabilities when working in UDP mode are reduced compared to TCP mode.

The table below lists the actions available depending on the mode that you are using.

Available actions when working together with EPP applications

Action	TCP mode	UDP mode
Registering events based on EPP technology (workstation and server protection events)	✓	✓
Populating the table of devices with devices hosting installed EPP applications (and devices that have had bidirectional interactions with such devices)	✓	✓
Updating the table of devices with information about devices hosting installed EPP applications (for example, the operating system version, information on the model or developer)	✓	✓
Displaying special icons on the nodes of the network interaction map and the nodes of topology map, that indicate the presence and the connection state of EPP applications	✓	✓
Network session registration	✓	✓
Monitoring device equipment	✓	—
Monitoring device users	✓	—
Monitoring device applications and patches	✓	—
Device configuration control	✓	—
Executable file launch control on devices	✓	—
Scanning devices as a part of vulnerability and compliance audit jobs and configuration control jobs	✓	—
Triggering response actions when logging events using the EPP technology, if threat development chains are built for these events in Endpoint Agent	✓	—

You can watch the tutorial video (see below) to familiarize yourself with the functionality.

https://www.youtube.com/watch?v=vp8THStYF84

SPAN-less mode

The HTTPS over TCP protocol is used to securely connect computers running Endpoint Agent to integration servers in TCP mode. HTTP connections are secured by using certificates issued by the Kaspersky Industrial CyberSecurity for Networks Server. The following certificates can be used in TCP mode connections:

- Integration server certificate. This certificate is verified by the computer with Endpoint Agent each time a connection is established. A connection is not established until certificate verification is successfully completed.

- Client certificate. This certificate is used to authenticate integration server clients that are computers with Endpoint Agent. The same client certificate can be used by multiple computers with Endpoint Agent. By default, an integration server does not verify certificates of clients, but you can enable client certificate verification to reinforce the security of connections.

When working in UDP mode, it is recommended to ensure the protection of transmitted data by encrypting it. To encrypt data, computers running Endpoint Agent must use the encryption keys received from Kaspersky Industrial CyberSecurity for Networks.

Certificates and public keys (for TCP mode) or encryption keys (for UDP mode) are delivered to computers running Endpoint Agent via Kaspersky Security Center. To preload this data, Kaspersky Security Center uses communication data packages, which are archives containing the corresponding files. A communication data package must be created in Kaspersky Industrial CyberSecurity for Networks after adding an integration server.

Only users with the Administrator role can configure receipt of data from EPP applications.

Scenario for preparing to receive data from EPP applications

The scenario for preparing to receive data from EPP applications consists of the following phases:

1. **Installing EPP applications to computers of the monitored network**

   During this phase, you need to install Kaspersky applications that perform functions for protecting workstations and servers (EPP applications). EPP applications need to be installed on all computers whose data you want to receive in Kaspersky Industrial CyberSecurity for Networks. These computers must either reside outside of the industrial network (whose traffic is monitored through monitoring points) or have an additional connection to another network that includes one of the nodes that has a Kaspersky Industrial CyberSecurity for Networks component installed (for example, a connection to the Kaspersky Industrial CyberSecurity dedicated network).

   If the functions of the Endpoint Agent software component for EPP applications are performed by Kaspersky Endpoint Agent, this application must also be installed on the corresponding computers.

   > Kaspersky Industrial CyberSecurity for Networks supports integration with the following EPP applications: Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Linux Nodes. To find out the versions of supported EPP applications, please refer to the Hardware and software requirements article.

2. **Adding integration servers for nodes of Kaspersky Industrial CyberSecurity for Networks**

   This phase involves the completion of procedures for adding integration servers to the nodes that computers with the Endpoint Agent software component will connect to. Network interactions between nodes and these computers are possible only through network interfaces that are not being used as monitoring points. Specific network interfaces and IP addresses are not configured for integration servers because any available network interface and IP address of a computer can be used for an external connection to the integration server.

3. **Creating communication data packages for integration server clients**

At this phase, you need to create and download communication data packages in which the application saves certificates and/or keys for connections between clients and integration servers.

Each communication data package used to connect to Endpoint Agent computers in TCP mode is an archive containing the following data:

- Public certificate key of the integration server.
- Certificate for integration server clients (with private key). This certificate is added if client certificate verification is enabled on the integration server. The certificate and key are saved in encrypted form with the password that was specified when the communication data package was created.

In UDP mode, the communication data package is an archive containing the encryption key. The encryption key is saved in encrypted form with the password that was specified when the communication data package was created.

4. **Uploading integration server connection data to client computers**

   Computers with the Endpoint Agent software component serve as clients for Kaspersky Industrial CyberSecurity for Networks integration servers.

   At this stage, Kaspersky Security Center is used to upload data to client computers. To perform it, upload certificates and/or keys from communication data packages to the Kaspersky Security Center Administration Server by using the Endpoint Agent administration plug-in. After that, you can create policies in Kaspersky Security Center for uploading data to computers with Endpoint Agent. For information about working with data and creating policies, please refer to the documentation of the EPP application or the Kaspersky Endpoint Agent documentation. At least one policy must be created for each integration server.

5. **Enabling an integration server in the necessary mode**

   This phase is completed after applying policies and uploading data to computers with Endpoint Agent. During this phase, you must enable TCP and/or UDP modes for all integration servers to which the data from EPP applications will be transmitted. When the integration server is enabled, the following services are activated on the node:

   - kics4net-epp-proxy – when the integration server is enabled in TCP mode.
   - kics4net-telemetry-proxy – when the integration server is enabled in UDP mode.

6. **Additional configuration for receiving telemetry data via data diodes**

   This step is performed if computers running Endpoint Agent must send telemetry data to Kaspersky Industrial CyberSecurity for Networks via data diodes.

   Depending on the versions of the EPP applications, Endpoint Agent components can send telemetry data via data diodes using the following protocols:

   - MQTT over TCP.

     This protocol is used when working in integration mode with Kaspersky Industrial CyberSecurity for Nodes. To receive telemetry data over this protocol, TCP mode must be enabled on the integration server. For detailed information on configuring EPP applications for this data transfer method, please refer to the appropriate Help system: Kaspersky Industrial CyberSecurity for Nodes 4.5 or Kaspersky Endpoint Agent 4.0. To deliver MQTT messages via data diode, you may need to configure the MQTT broker functionality on the data diode side according to the manufacturer's documentation.

   - UDP

     This protocol is used when working in integration mode with Kaspersky Industrial CyberSecurity for Linux Nodes version 2.0. To receive telemetry data over this protocol, UDP mode must be enabled on the integration server. For detailed information on configuring EPP applications for this data transfer method, please refer to the Help system of Kaspersky Industrial CyberSecurity for Linux Nodes 2.0.

It is also recommended to perform the following steps to configure the nodes and network equipment:

- Specify the IP and MAC addresses of the nodes hosting the integration servers in the ARP tables on the computers running EPP applications.
- When using backup networks, assign IP addresses not affiliated with any backup network to the nodes hosting integration servers.
- Specify static routes to nodes hosting integration servers in the routing tables on nodes running EPP applications.
- After each switchover to the backup network on nodes running EPP applications, stop and restart the Kaspersky Industrial CyberSecurity for Networks integration task by running the following commands:

  ```
  sudo kics-control --stop-task 23
  sudo kics-control --start-task 23
  ```

- In the configuration of each data diode, increase the value for Maximum Transmission Unit (MTU) to 1514 bytes.
- In the configuration of each network switch located between the nodes running EPP applications and the data diode, add the static addresses of the nodes hosting integration servers to the MAC address table. The node MAC address must be specified for the outbound port on the network switch.

When this scenario is fulfilled, Kaspersky Industrial CyberSecurity for Networks will begin to receive and process data from EPP applications.

Adding an integration server

To add an integration server:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection servers**.
3. On the **Integration servers** tab, open the details by clicking **Add Endpoint Agent integration server**.
4. In the **Node** drop-down list, select the node with the installed application component (Server or sensor) to which you need to add an integration server.

   You can only select a node that does not yet have an added integration server.
5. If you need to enable certificate verification for client authentication when operating in TCP mode, create one or more certificates for integration server clients. To do so, click the **Create new certificate** button in the **Certificates for clients (TCP mode)** section.

   You can create 10 certificates for integration server clients. If necessary, you can remove unnecessary certificates from the list by using the × icon located on the right of the field containing the certificate fingerprint.

   If you created multiple client certificates, you can select the relevant certificate when creating the communication data package.

6. If you need to receive encrypted data from EPP applications when operating in UDP mode, create one or more encryption keys. To do so, click the **Create encryption key** button in the **Encryption keys (UDP mode)** section.

   You can create 10 encryption keys. If necessary, you can remove unnecessary keys from the list by using the × icon located on the right of the field containing the key fingerprint.

7. Click **Save**.

Creating a communication data package for integration server clients

After adding an integration server or changing its settings, you need to create and download a communication data package for clients of this server.

To create a new communication data package for integration server clients:

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

2. Select **Settings** → **Connection servers**.

3. On the **Integration servers** tab, select the server for whose clients you want to create a new communication data package.

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

4. Click the **Get communication data package** button.

5. If client certificate verification or encryption of transmitted data is enabled for the integration server, the **Generating a new communication data package** window opens. Perform the following actions:

   a. Do one of the following:

      a. If you need to configure a secure connection with integration server clients using HTTPS over TCP, select **Connection type** from the **TCP** drop-down list and then select the necessary certificate to be used for integration server client authentication from the **Certificate for clients** drop-down list.

      b. If you need to receive encrypted data from EPP applications using UDP, select **Connection type** from the **UDP** drop-down list and then select the necessary encryption key to use for data encryption from the **Encryption key** drop-down list.

   b. Specify the password for accessing the selected certificate or encryption key. Using the defined password, the certificate or encryption key will be encrypted in the communication data package.

   c. Click **Create communication data package**.

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

You will need to upload the contents of the new communication data package to the computers of integration server clients. These uploads are performed by using Kaspersky Security Center Administration Server policies. In the Kaspersky Security Center policies, you need to specify the IP address for connecting to the integration server (to do so, you can use one of the available IP addresses indicated in the details area of the selected integration server).

Kaspersky Security Center policies are created and configured while configuring the integration with the EPP application. For information about configuring integration, please refer to the documentation of the EPP application or the Kaspersky Endpoint Agent documentation.

Integration servers table

The integration servers table is displayed under **Settings** → **Connection servers** on the **Integration servers** tab. This table displays information about integration servers that were added to nodes that have application components installed.

The integration servers table contains the following information:

- **Node name** – name of the node that has the application component installed.
- **IP addresses** – list of IP addresses on all network interfaces of the node (specific network interfaces and IP addresses are not configured for integration servers because any available network interface and IP address of a computer can be used for an external connection to the integration server).
- **TCP mode** – current status of integration server operation in TCP mode.
- **Verify client certificate** – indicator of whether client certificate verification is enabled or disabled in TCP mode (if verification is disabled, the table cell is empty).
- **Requests per second** – average number of successfully processed requests coming from clients to the integration server.
- **UDP mode** – current status of integration server operation in UDP mode.
- **Encryption for UDP** – indicator of whether encrypted data reception is enabled or disabled when operating in UDP mode (if encrypted data reception is disabled, the table cell is empty).

Enabling and disabling an integration server in the necessary mode

An integration server can operate in TCP and UDP modes. TCP and UDP modes are disabled by default after the integration server is created. Therefore, data from clients of this server is not processed in Kaspersky Industrial CyberSecurity for Networks.

You can use TCP and UDP modes either separately or simultaneously.

To enable or disable connections to computers running Endpoint Agent:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connection servers**.
3. On the **Integration servers** tab, select the server for which you want to enable or disable connections to EPP applications.

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

4. If you need to enable or disable the integration server in TCP mode, click the **Enable TCP mode** or **Disable TCP mode** button.

5. If you need to enable or disable the integration server in UDP mode, click the **Enable UDP mode** or **Disable UDP mode** button.

Editing integration server settings

When editing integration server settings, you can replace the certificate for the integration server itself or edit the list of certificates and encryption keys for clients.

To edit the integration server settings:

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

2. Select **Settings** → **Connection servers**.

3. On the **Integration servers** tab, select the server for whose clients you want to change the settings.

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

4. Click **Edit**.

5. If you want to replace (issue a new) certificate for the same integration server, click **Reissue certificate**.

   After the integration server certificate is replaced, its old certificate becomes invalid.

6. If you want to modify the list of certificates for clients in TCP mode, click **Create new certificate** and/or the × icon located on the right of the field containing the certificate fingerprint.

7. If you want to edit the list of encryption keys for computers running Endpoint Agent in UDP mode, use the **Create encryption key** button and/or the × icon that is located on the right of the field containing the key fingerprint.

8. Click **Save**.

If a new certificate was issued for an integration server or if new client certificates or encryption keys were created, you need to once again create and download a communication data package to send data about these certificates and/or encryption keys to client computers.

Removing an integration server

You can remove an integration server that has been added. After removing the integration server, Kaspersky Industrial CyberSecurity for Networks will no longer receive data from linked EPP applications.

To remove an integration server:

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

2. Select **Settings** → **Connection servers**.

3. On the **Integration servers** tab, select the server that you want to remove.

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

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Managing response actions in Kaspersky Industrial CyberSecurity for Networks

If joint operation with EPP applications is configured in Kaspersky Industrial CyberSecurity for Networks, you can trigger the response actions on devices. Response actions allow preventing or minimizing the consequences of detected threats from devices in an industrial network. Each response action is triggered manually when working with the corresponding object in the application.

The capability to trigger response actions is available for devices with the Endpoint Agent software component. When a response action is triggered, Kaspersky Industrial CyberSecurity for Networks transmits the information about it to Endpoint Agent. The Endpoint Agent software component executes the received command and sends a completion notification to Kaspersky Industrial CyberSecurity for Networks.

Depending on the nature of the threats detected on devices, you can trigger the following response actions:

- **Isolate device from the network**.

  After enabling network isolation of a device, the Endpoint Agent software component terminates all active TCP/IP network connections on the device and blocks all new ones, except for the following connections:

  - Connections excluded from network isolation in Endpoint Agent.
  - Connections initiated by services of the EPP application compatible with Endpoint Agent.
  - Connections initiated by Endpoint Agent services.
  - Connections initiated by Kaspersky Security Center Network Agent.

  Device network isolation remains active until network isolation is disabled in Kaspersky Industrial CyberSecurity for Networks. If network isolation is not manually disabled, it will be disabled automatically 9999 hours after it is enabled.

- **Prevent run**.

  You can configure rules to block the launch of executable files and scripts, as well as the opening of office format files on selected devices. For example, you can block the launch of applications that you consider insecure on a selected device running the Endpoint Agent software component. The application identifies files by their file path or checksum using the MD5 and SHA256 hashing algorithms.

  In the event of launch blocking, the user is notified about the triggered launch blocking rule. If the device user does not close the pop-up notification, it will close automatically 60 seconds after it appears.

- **Move to quarantine**.

  Quarantine is a designated local storage on a device running the Endpoint Agent software component that stores files potentially infected with viruses or that were incurable at the time of detection. Quarantined files are stored encrypted and do not create a threat to the device security.

Kaspersky Security Center generates a common list of quarantined objects on devices running Endpoint Agent. Device Network Agents transmit information on quarantined files to the Administration Server.

Kaspersky Security Center Network Agent does not copy quarantined files to the Administration Server. All objects are located on protected devices running Endpoint Agent. Objects are restored from quarantine on protected devices.

- **Delete file**.

  System-critical objects (SCOs) cannot be deleted. SCOs are files that are required for proper operation of the operating system and the EPP application.

  Deletion of a file from the device file system may be postponed until the device is restarted (for example, if the file is being used by other processes). If file deletion is postponed until the device is restarted, the EPP application notifies Kaspersky Industrial CyberSecurity for Networks about this. In this case, after the response action is triggered, Kaspersky Industrial CyberSecurity for Networks displays a warning about the postponed file deletion. It is recommended to check whether the file was successfully deleted after the device is restarted.

- **Terminate process**.

  You can remotely terminate processes running on the device. The EPP application terminates the process that is started from the file at the file path specified for the response action. The characters in the process name are case sensitive (the process name must fully match the file name in the response action).

  System-critical objects (SCOs) cannot be terminated.

  The device may have multiple processes running at the file path specified for the response action. In this case, the EPP application tries to terminate all such processes, taking into account the limit on the number of processes that can be terminated (if such a limit is specified in the application). Therefore, if there is a large number of processes running from a single executable file, the EPP application may not be able to terminate some of these processes.

- **Start process**.

  On the device, you can remotely run processes of executable files (including processes that were terminated via the **Terminate process** response action), scripts, utilities, and applications. To start a process, you must specify the start command. You can also specify command-line arguments and the path to the working directory. Note that to start a process using the Kaspersky Industrial CyberSecurity for Linux Nodes EPP application on the device, you may need to configure the SELinux system.

  After the command is executed, the Endpoint Agent software component sends text files containing data from the standard output and error streams to Kaspersky Industrial CyberSecurity for Networks when the process is started (no more than 100 KB of data in each file).

For the **Isolate device from the network**, **Prevent run** and **Move to quarantine** response actions, you can trigger the corresponding reverse actions in Kaspersky Industrial CyberSecurity for Networks. This capability allows you to restore normal device functionality after a triggered response action has been completed and the threat has been eliminated from the device. The following reverse actions are available:

- **Disable network isolation**.
- **Disable run prevention**.
- **Restore from quarantine**.

Kaspersky Industrial CyberSecurity for Networks registers triggered response actions and the corresponding reverse actions. The registered actions are displayed in the **Events** section on the **Response actions** tab.

You can trigger response actions by selecting the relevant events, executable files or devices. You can also trigger new response actions by using ones that were registered and completed as long as the selected action allows triggering reverse actions.

The actions available to you depend on the selected object. For example, if you selected a device with the Endpoint Agent software component, you can only manage the network isolation of this device and the startup of processes. All other response actions are available under other conditions.

Only users with the Administrator or Security Officer role can trigger response actions and corresponding reverse actions.

Triggering event response actions

You can trigger response actions on a device using a registered event that is associated with such device. To trigger a response action, an event must be registered using EPP technology and a threat development chain must be built for this event in Endpoint Agent (the event is an EDR incident).

Triggering a response action for a device in an EDR incident: **Isolate device from the network**

You can trigger the **Isolate device from the network** response action for any EDR incident.

To isolate a device associated with an EDR incident from the network:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Events and incidents** tab in the **Events** section.
3. In the table of events, select the relevant event that is an EDR incident.

   The details area appears in the right part of the web interface window.
4. In the details area, open the **Threat response** drop-down list and select **Isolate device from the network**.

   A window with a confirmation prompt opens.
5. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering a response action for an object in an EDR incident activity event: **Prevent run**, **Move to quarantine**, **Delete file**, or **Terminate process**.

For EDR incidents that have activity events of the **File creation** or **Starting a process** type in the threat development chain, you can trigger the **Prevent run**, **Move to quarantine**, or **Delete file** response actions. Additionally, for activity events with the **Starting a process** type, the application provides the capability to trigger the **Terminate process** response action.

For the specified activity event types, you can use the following options for triggering response actions:

- Trigger for threat detection object in key activity event: the response action is applied to a threat detection object from a key activity event of a supported type.
- Trigger for any activity event of a supported type: the response action is applied to an object from the selected activity event in the threat development chain.

To trigger a response action for a threat detection object:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Events and incidents** tab in the **Events** section.
3. In the table of events, select the relevant event that is an EDR incident.

   The details area appears in the right part of the web interface window.
4. In the details area, open the **Threat response** drop-down list and select the appropriate item:

   - If the activity event with the threat detection object has the **File creation** type, the following response action items are available for selection: **Prevent run**, **Move to quarantine**, and **Delete file**.
   - If the activity event with the threat detection object has the **Starting a process** type, the following response actions are available for selection: **Prevent run**, **Move to quarantine**, **Delete file**, and **Terminate process**.

   A window with a confirmation prompt opens.
5. If a response action requires you to confirm the operation using your password, enter your password.
6. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

To trigger a response action for any activity event of a supported type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Events and incidents** tab in the **Events** section.
3. In the table of events, select the relevant event that is an EDR incident.

   The details area appears in the right part of the web interface window.
4. In the details area, go to the **All activity events** tab and select the appropriate activity event.

   You can select any activity event with the **File creation** or **Starting a process** type. A key activity event (with a threat detection object) is marked with the **Detection** icon.

5. In the activity event details window that opens, click the appropriate button:

   - If an activity event of the **File creation** type is selected, buttons with the **Prevent run**, **Move to quarantine**, and **Delete file** response actions are available.
   - If an activity event of the **Starting a process** type is selected, buttons with the **Prevent run**, **Move to quarantine**, **Delete file**, and **Terminate process** response actions are available.

   A window with a confirmation prompt opens.

6. If a response action requires you to confirm the operation using your password, enter your password.
7. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering a response action for a device in an EDR incident: **Start process**

You can trigger the **Start process** response action for any EDR incident.

To start a process on a device linked to an EDR incident:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Events and incidents** tab in the **Events** section.
3. In the table of events, select the relevant event that is an EDR incident.

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

4. In the details area, open the **Threat response** drop-down list and select **Start process**.

   This opens the window for configuring the response action.

5. Configure the settings for running the process on the device. To do so, enter values for the following settings:

   - Full path to the executable file, script, utility, or application.
   - Working directory (optional).
   - Additional startup keys (optional).

6. Enter your password in the **Operation confirmation password** field.
7. Click **Run**.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering response actions when working with device executable files

You can trigger response actions for an executable file, information about which was received during launch control of executable files on devices. To trigger a response action, the executable file must be associated with a device that has the Endpoint Agent software component and is prepared to receive data from EPP applications.

When working with the table of executable files, you can trigger the following response actions:

- **Prevent run**.
- **Move to quarantine**.
- **Delete file**.
- **Terminate process**.

To trigger a response action for an executable file:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Executable files** tab in the **Assets** section.
3. In the executable files table, select the file you need.

   The details area appears in the right part of the web interface window.
4. In the details area, open the **Threat response** drop-down list to trigger the required response action.

   Items in the **Threat response** drop-down list are available if the Endpoint Agent software component is installed on the device associated with the executable file.

   A window with a confirmation prompt opens.
5. If a response action requires you to confirm the operation using your password, enter your password.
6. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering device response actions

You can trigger the **Isolate device from the network** response action and the corresponding reverse action **Disable network isolation**, and the **Start process** action on a device. To trigger a response action, the device must run the Endpoint Agent software component and must be prepared to receive data from EPP applications.

To trigger a network isolation action for a device:

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

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device on both the network interaction map and the topology map.

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

3. In the details area, open the **Threat response** drop-down list and select the appropriate item:

   - **Isolate device from the network** – if you want to isolate the selected device from the network.
   - **Disable network isolation** – if you want to disable network isolation of a device for which the **Isolate device from the network** action was previously triggered.

   Items in the **Threat response** drop-down list are available if the Endpoint Agent software component is installed on the device.

   A window with a confirmation prompt opens.

4. In the request window, confirm the start of the response action.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

To start a process on a device:

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

2. Select the device in the **Assets** section on the **Devices** tab or in the **Network map** section.

   In the **Network map** section, you can select the device on both the network interaction map and the topology map.

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

3. In the details area, open the **Threat response** drop-down list and select **Start process**.

   Items in the **Threat response** drop-down list are available if the Endpoint Agent software component is installed on the device.

   This opens the window for configuring the response action.

4. Configure the settings for running the process on the device. To do so, enter values for the following settings:

   - Full path to the executable file, script, utility, or application.
   - Working directory (optional).
   - Additional startup keys (optional).

5. Enter your password in the **Operation confirmation password** field.

6. Click **Run**.

The application will register a new response action. You can view information about this action in the **Events** section on the **Response actions** tab.

Triggering response actions when working with registered response actions

If the Isolate device from network**Isolate device from the network**Prevent run**Prevent run**Move to quarantine**Move to quarantineresponse action** was triggered in Kaspersky Industrial CyberSecurity for Networks, you can trigger the corresponding reverse action in the **Events** section on the **Response actions** tab. For example, if the **Isolate device from the network** action is triggered for a device, you can trigger the **Disable network isolation** action for this device when working with registered actions.

After registering a reverse action, you can use it to trigger the next response action for the same device or object. For example, if you want to isolate a device from the network again after disabling the network isolation.

For the **Disable run prevention** and **Restore from quarantine** registered actions, you can trigger both **Prevent run** and **Move to quarantine** as a reverse action.

To trigger a response action that is reverse in respect of a registered action:

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

2. Select the action on the **Response actions** tab in the **Events** section.

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

3. In the details area, click the reverse action start button. For example, if you selected the **Isolate device from the network** action, click **Disable network isolation** to trigger the reverse action.

   The buttons for triggering reverse actions are available if one of the following response actions is selected:

   - **Isolate device from the network**.
   - **Prevent run**.
   - **Move to quarantine**.
   - **Disable network isolation**.
   - **Disable run prevention**.
   - **Restore from quarantine**.

   A window with a confirmation prompt opens.

4. In the request window, confirm the start of the response action.

The application will register a new response action.

Viewing the response action table

The response actions table is displayed on the **Response actions** tab in the **Events** section. The table shows the response actions that are registered when the response actions are triggered in Kaspersky Industrial CyberSecurity for Networks.

Response action settings are displayed in the following columns of the table:

- **ID**

  Unique ID of the registered action.

- **Start**

  Action start date and time.

- **End**

  The date and time when the action was completed or a confirmation of the action was received. If the application has not received a confirmation of the action, the date and time when the time-out period expires for the action to be performed is displayed.

- **Action type**

  The type of the registered action. The following types are provided:

  - **Isolate device from the network**.
  - **Prevent run**.
  - **Move to quarantine**.
  - **Disable network isolation**.
  - **Disable run prevention**.
  - **Restore from quarantine**.
  - **Delete file**.
  - **Terminate process**.
  - **Start process**.

- **Status**

  Action completion status. The following statuses are available:

  - **Pending** – a command to start the action has not been sent yet.
  - **Running** – the action is being started or is in progress.
  - **Success** – the action is completed successfully.
  - **Failure** – an error occurred when performing the action or the action was canceled due to expiry of the period for receiving a confirmation.

- **Device**

  The name of the device for which the action was triggered.

- **Event title**

  The event title if the action was triggered while working with the event.

- **Object type**

  The type of an object for which the action was triggered.

- **Object**

  The name of the object for which the action was triggered.

When viewing the response action table, you can use configuration, filter, search and sort functions, and navigate to the related items.

Downloading files containing data from the standard output and error streams when starting a process

After the **Start process** response action is successfully completed, the Endpoint Agent software component sends stdout and stderr text files containing data from the standard output and error streams to Kaspersky Industrial CyberSecurity for Networks when the process is started. Files are sent if the corresponding data was received on the device.

There is a data size limit for sent files. If the source file size is greater than 100 KB, the Endpoint Agent software component removes some of the data in the sent file to reduce the file size to 100 KB.

When downloading stdout and stderr files, you must consider the following:

- Files containing process startup data are stored in the Server database temporarily and are automatically deleted after seven days in storage.
- Users with the Administrator or Security Officer role can download files.

To download a file containing standard output or error stream data:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the action on the **Response actions** tab in the **Events** section.

   The details area appears in the right part of the web interface window.
3. In the details area, open the **Download data** drop-down list and select the relevant item: **Standard output stream (stdout)** or **Standard error stream (stderr)**.

   The drop-down list and items are available if the **Start process** response action is selected and the files containing the corresponding data are stored in the Server database.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Deleting response actions

You can delete registered response actions. However, you cannot delete actions with the *In progress* status.

Before deleting a response action, the application checks the current status of this action. However, during and after deletion of an action, the application does not monitor the operations for this action performed on the device and does not cancel operations if they have already started. As a result, a response action may be performed on the device even if this action had the **Pending** status at the time of deletion.

Deleting a registered action does not override the result of the action performed on the device. For example, if a successfully completed **Isolate device from the network** action is deleted, network isolation of the device continues after the action is deleted. To disable network isolation, the **Disable network isolation** action must be triggered.

After deleting the **Start process** response action in Kaspersky Industrial CyberSecurity for Networks, the standard output and error stream files that were received when the action was performed are also deleted.

To delete a response action:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the action on the **Response actions** tab in the **Events** section.
3. Click **Delete**.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm the deletion of the action.

Managing connectors

This section contains information about managing connectors in Kaspersky Industrial CyberSecurity for Networks. *Connectors* are specialized application modules that facilitate the exchange of data with Kaspersky Industrial CyberSecurity for Networks and may provide capabilities to perform management tasks in the application directly or through use of the application.

Connectors expand application functionality for interaction with recipient systems, including with Kaspersky Security Center. Depending on their functional purpose, connectors can transmit data to recipient systems (for example, relay events, application messages and audit entries to a SIEM system) or receive data from recipient systems (for example, to register External events in the application). The application may also use connectors to conduct active polling of devices.

A specialized connector named **Kaspersky Security Center Connector** is used so that the application can interact with Kaspersky Security Center. This connector is created in the application by default and cannot be deleted. To ensure proper functioning of the connector, the capability for the application to interact with Kaspersky Security Center must be added to the Kaspersky Industrial CyberSecurity for Networks Server.

Computers running application modules of connectors are called *connector deployment nodes*. A connector deployment node can be any computer that has network access to the application Server computer (such as nodes that have application components installed, including the actual computer of the Server).

The functional capabilities of the connector depend on the selected *connector type*. You can select the relevant connector type when adding a connector to the application. The application has the following built-in connector types by default:

- **Syslog**

  This connector type enables data forwarding to a Syslog server.

  When adding a **Syslog** connector or changing its settings, configure both the general settings of the connector, and the additional settings under **Details**:

  - Syslog server address
  - Syslog server port
  - Data transfer systems

- **SIEM**

  This connector type enables data forwarding to a SIEM system.

  When adding a **SIEM** connector or changing its settings, configure both the general settings of the connector, and the additional settings under **Details**:

  - SIEM system server address
  - SIEM system server port
  - Data transfer protocol

- **Generic**

  This connector type provides the capabilities for connecting applications that utilize the Kaspersky Industrial CyberSecurity for Networks API.

- **Email**

  This connector type provides the capabilities for forwarding data by email.

  When adding an **Email** connector or changing its settings, configure both the general settings of the connector, and the additional settings under **Details**:

  - Address indicated as the sender of email messages.
  - Recipient addresses of email messages.
  - Subjects of email messages for events, application messages, and audit entries.
  - Templates of text descriptions for events, application messages, audit entries, network interactions, and for entire messages containing notifications. Templates are formed by using variables.
  - Subject and text of an email message notifying when the maximum number of sent notifications is reached.

- Maximum number of email messages sent per day.
- Maximum number of notifications in each message. Defines the maximum number of registered notifications of one type (events, application messages, or audit entries) that can be put into one email message. If the number of registered notifications exceeds the maximum number, an additional email message is generated (within the daily limit).

- **Active poll**

  This connector type provides the capabilities for active device polling with configuration control and active polling jobs.

  When adding an **Active poll** connector or changing its settings, configure both the general settings of the connector, and the additional settings under **Details**:

  - Active polling methods that will be available to the application user when using the connector.
  - The ranges of allowed and denied IP addresses of the devices for which active polls are allowed or denied. The address `0.0.0.0` corresponds to all possible IP addresses. If an address is included in the range of both allowed and denied IP addresses, Kaspersky Industrial CyberSecurity for Networks treats it as a denied IP address.
  - Names of address spaces whose corresponding devices will be available for active polling. If necessary, select the address spaces for IP addresses in the **L3 address space** field and select the address spaces for MAC addresses in the **L2 address space** field.

    If you select an address space that differs from the **Default** one, add a new rule for this address space (or change the existing rule). The rule must specify the connector for which this address space is selected. The rules settings are configured when the address space is changed.

- **KUMA**

  This connector type provides integration with Kaspersky Unified Monitoring and Analysis Platform (KUMA). Software modules for this type of connectors are supplied separately from Kaspersky Industrial CyberSecurity for Networks. Using this type of connector, you can send information about devices and risks to KUMA, as well as use the commands to change device statuses in KUMA. After adding the connector, configure the integration in KUMA (create a connection to Kaspersky Industrial CyberSecurity for Networks). Interaction between the KUMA connector and the Server is performed using the Kaspersky Industrial CyberSecurity for Networks API.

  The KUMA connector provides integration by sending information about devices and risks and applying commands to change device statuses. To send events to KUMA, add a **Syslog** or **SIEM** connector to Kaspersky Industrial CyberSecurity for Networks and specify the data for connecting to the KUMA server for this connector. After adding a connector, configure the collector on the KUMA side.

- **Cisco Switch**

  This connector type provides support for automatic network access control for devices via Cisco network switches.

  When adding a **Cisco Switch** connector or changing its settings, configure both the general settings of the connector, and the additional settings under **Details**:

  - Switch name to use in the application event log that records actions involving the connector.
  - Addressing information for connecting the connector to the switch: IP address and SSH port.
  - Credentials for connecting to the switch via SSH.

- Public key used for verification of matches with the received public key of the network switch before establishing an SSH connection to protect against spoofing of this device in the network (if the value is empty, the verification is not performed).

- Method used to restrict network access for devices. The application provides methods for creating deny rules in switch access control lists based on MAC addresses (MAC ACL), IP addresses (IP ACL), and by disabling Ethernet ports to which devices are connected.

  To use the method of disabling Ethernet ports, configure the switch connections to prevent multiple devices from being connected to one port. Otherwise, disabling an Ethernet port to block one device will also block network access for all devices that connect to the network using that port.

- Option that controls whether deny rules are reset when the method of restricting network access changes. If the option is enabled, changing the method resets previously defined deny rules.

- Option that controls exclusions from network access restrictions for **Network devices**, **Firewalls**, **Switches**, **Virtual switches**, **Routers**, **Virtual routers**, and **Wi-Fi**. If the option is enabled, these categories of devices are excluded from the access restriction method.

- Option that controls whether deny rules are applied to new devices only. If the option is enabled, the method is applied only to those unauthorized devices for which a new 4000005003 device detected event has been registered.

- Polling interval for *Authorized* and *Unauthorized* devices in the table of devices.

- Setting that controls whether to send notifications about blocked devices when the connector restarts. If the option is enabled, after the connector turns on or restarts, the application sends a list of devices to which network access restrictions have been applied to the Server.

If necessary, you can add other connector types that will facilitate data exchange or provide the capabilities for performing management tasks when the application interacts with other recipient systems.

Certain ports and protocols are used to connect the connectors to the Server.

A recipient system is connected through a connector on behalf of one of the application users. It is recommended to use a separate user account for each connector. This will make it more convenient to analyze the actions that are performed through connectors based on audit entries.

The connectors table and connector types table are displayed under **Settings** → **Connectors** in the application web interface. Only users with the Administrator role can manage connectors and connector types.

Maximum number of connectors in the application – 20. Maximum number of connector types – 100.

About manageable and unmanageable connectors

Manageable and unmanageable connectors can be used in the application.

A connector is *manageable* if its application modules can access functions for automatic registration and startup after the connector is added, and can access functions for managing these modules when enabling or disabling the connector or when deleting it. Only nodes that have application components installed can serve as deployment nodes for manageable connectors.

An *unmanageable connector* does not provide the functions of a manageable connector. Registration of this type of connector, and startup, stoppage, and deletion of its application modules must be performed manually on the connector deployment node. When an unmanageable connector is enabled or disabled, interaction with this connector on the Server side is allowed or blocked, respectively.

The connections between connectors and the application Server are secured by using certificates. Certificates are created for connectors when these connectors are added to the application. The application automatically forwards the created certificates for application modules of manageable connectors. When adding an unmanageable connector (or when adding a manageable connector configured to ignore the functions of a manageable connector), the certificate for application modules of this connector must be manually uploaded using a communication data package. If you need to replace (issue a new) certificate for this type connector, you must create a new communication data package and use this file to upload the new certificate. Certificates of manageable connectors can be replaced only by deleting these connectors and then adding them again.

About forwarding events, application messages and audit entries to recipient systems

You can configure forwarding of events, application messages, or audit entries (hereinafter also referred to as "registered notifications") to a recipient system by using connectors. For the connector types named **Syslog**, **SIEM**, **Email**, and **Kaspersky Security Center Connector**, the capability to forward registered notifications is enabled by default. For the KUMA **connector type**, the capability to forward registered notifications is available if application modules are installed. When using other connector types that were added to the application, this capability is available depending on the settings defined for these specific connector types.

The settings for forwarding registered notifications are configured for each connector individually. When configuring event types, you can select the relevant event types to forward via connectors. When creating a connector or changing its settings, you can enable or disable forwarding of all application messages and all audit entries through this connector.

Some connector types provide the capability to limit the volume of transmitted data. This limit is applied for a 24-hour period starting at 0:00 in the time zone of the Server. You can set a limit on the volume of transmitted data for the following system types of connectors:

- **Email**. For this type of connector, you can define the maximum number of email messages regarding new registered notifications and the maximum number of registered notifications in each message. If the maximum number of email messages has been sent, message recipients receive one more message notifying them that the maximum number has been exceeded. After this, new messages will not be sent until the end of the current day.

- **Kaspersky Security Center Connector**. For this type of connector, you can define the maximum number of registered notifications that can be forwarded. If the number of registered notifications exceeds this maximum number, the excess notifications registered before the end of the current day are not sent to Kaspersky Security Center.

Events containing information about multiple network interactions are specially forwarded as follows. Each of these events is considered as one item when forwarded through the **Kaspersky Security Center Connector**. However, when it is being forwarded, the event is converted into multiple registered notifications, with each notification representing one network interaction. For this reason, the list of registered notifications for the **Kaspersky Security Center Connector** may contain more notifications than defined by the setting that determines the maximum number of notifications.

The contents and order of information about registered notifications forwarded through **Syslog** and **SIEM** connectors may differ from the contents and order of information displayed on pages of the Kaspersky Industrial CyberSecurity for Networks web interface.

Email messages forwarded through an **Email** connector are generated separately for each type of registered notification. In other words, separate email messages are generated to forward events, application messages, and audit entries.

Automatic network access control for devices via Cisco Switch connectors

You can configure automatic network access control for devices via **Cisco Switch** connectors. Connectors of this type interface with switches to send commands that add or remove network access deny rules (restrictions) for the devices connected to the switches.

Network access control for devices is driven by their status. The connector creates deny rules on the switch for devices with a status of *Unauthorized* and removes the rules once the *Authorized* status is assigned to the devices.

Each connector can only interface with one network switch.

A **Cisco Switch** connector is used for restricting network access only for those devices whose details include their MAC addresses. Also, these MAC addresses must be stored in the ARP table of the network switch. That is, devices with these MAC addresses must be connected to the network switch to which the connector is connected.

A connector can use various methods to restrict network access for devices. The application provides methods for creating deny rules in switch access control lists based on MAC addresses (MAC ACL), IP addresses (IP ACL), and by disabling Ethernet ports to which devices are connected.

To use the method of disabling Ethernet ports, configure the switch connections to prevent multiple devices from being connected to one port. Otherwise, disabling an Ethernet port to block one device will also block network access for all devices that connect to the network using that port.

To minimize the risks of the connector impacting network accessibility for legitimate process devices, you can enable the following settings during configuration:

- Option that controls exclusions from network access restrictions for **Network devices**, **Firewalls**, **Switches**, **Virtual switches**, **Routers**, **Virtual routers**, and **Wi-Fi**. If the option is enabled, these categories of devices are excluded from the access restriction method.

- Option that controls whether deny rules are applied to new devices only. If the option is enabled, the method is applied only to those unauthorized devices for which a new 4000005003 device detected event has been registered.

The connector interfaces with the network switch via SSH. SSH connection credentials are specified and stored within the connector configuration. To protect these sensitive credentials, which are essential for identification and authentication, the connector verifies the switch public key it receives against a stored value as a safeguard against switch spoofing. Identification and authentication details are sent to the switch after verifying that the received public key matches the public key saved in the connector.

During the operation, the connector logs events in the application based on the results of the actions performed. These events are logged via External technology. The following event headers are generated:

- `Reset device deny rules for <switch name>`

  This type of event is logged when the connector resets previously defined deny rules for devices due to a change of network access restriction method.

- `Updated information about <device name> with address <device MAC address> according to data from <switch name>`

  This type of event indicates that the connector has received information from a switch that a device connected to a certain port.

- `Added a device deny rule for <device name> on <switch name>`

  This type of event is logged when the connector restricts network access for an unauthorized device.

- `Removed deny rule for <device name> on <switch name>`

  This type of event is logged when the connector has successfully removed network access restrictions for a specific device.

- `<switch name> has previously added deny rules`

  This type of event indicates that upon turning on or restarting, the connector discovered preexisting deny rules on a specific switch.

- `SSH connection made to <switch name> without verifying public key`

  This type of event is logged when the connector successfully establishes an SSH connection to a switch but fails to verify its public key. We recommend verifying that there is no spoofed device on the network, and then saving the new public key in the connector settings.

- `Detected public key mismatch for <switch name>`

  This type of event is logged when the connector detects a mismatch between the stored and received public keys for a switch. This prevents an SSH connection with the switch. We recommend verifying that there is no spoofed device on the network and that the switch public key has indeed changed, and then saving the new public key in the connector settings.

- `Failure to establish SSH connection with switch <switch name>: incorrect credentials`

  This event is logged when the connector failed to establish SSH connection with the switch due to incorrect credentials specified in the connector settings (user name and/or password).

- `Action for privileged mode was not performed on switch <switch name>: incorrect password`

  This event is logged when the connector does not have privileged mode capabilities to add and remove device deny rules on the switch. In this case, enter the correct privileged mode password in the connector settings.

Adding a connector

You can add a connector based on one of the connector types that are available in the application.

To use all KUMA integration capabilities, add two types of connectors. To send information about devices and risks to KUMA and use the commands to change device statuses, add a **KUMA** connector. To send Kaspersky Industrial CyberSecurity for Networks events to KUMA, add a **Syslog** or **SIEM** connector and specify the data for connecting to the KUMA server for this connector.

Prior to adding a connector, you are advised to create a separate user account that the recipient system will use to connect to the application.

To add a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, open the details area by clicking **Add connector**.
4. Configure the connector general settings:
   a. Select the relevant connector type and enter the connector name.
   b. If you want to add an unmanageable connector (or a connector configured to ignore the functions of a manageable connector), enter the password for accessing the connector certificate.

      Using the defined password, the certificate will be encrypted in the communication data package of the connector.
   c. Specify the address of the application Server.

      The connector will connect to the Server at the specified address.
   d. Specify the connector deployment node:
      - If you want to add a manageable connector, you can use one of the nodes that have application components installed as the connector deployment node.
      - If you want to add an unmanageable connector, you need to enter the IP address of the computer where the connector application modules will be running.
   e. Select the user account that the recipient system will use to connect to the application through the connector. You must indicate the name of one of the application users.
5. In the **Details** block, specify the advanced settings depending on the type of connector. The **Details** block is not shown in the details area if the connector type does not allow configuration of advanced settings.

6. If the connector type provides the capability to forward application messages and audit entries, use the corresponding check boxes to enable or disable forwarding of this data.

   Audit records cannot be transferred if the user who connected via the connector has the Operator role.

7. Enter a connector description if necessary.

8. Click **Save**.

   The new connector will appear in the connectors table.

   If an unmanageable connector was added, the Server generates a communication data package for the new connector. Then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file. You will need to upload the contents of the new communication data package to the application that will use the connector.

9. For an unmanageable connector, create a service on the node hosting the connector. To do so, you can use the corresponding script:

   - If a **Syslog**, **SIEM**, **Generic**, or **Email** connector has been added, you can create a service by using the default_connectors_registrar.py script located in the directory /opt/kaspersky/kics4net-connectors/libexec/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

     ```
     sudo python3 default_connectors_registrar.py create
     ```

     When prompted by the script to provide connector data, enter the name of the connector, the path to the communication data package, and the connector certificate access password.

   - If an **Active poll** connector has been added, you can create a service by using the register.py script located in the directory /opt/kaspersky/kics4net-apm/src/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

     ```
     sudo python3 register.py -p "<full path to the communication data package>"
     ```

Viewing the connectors table

The connectors table is displayed on the **Connectors** tab in the **Settings** → **Connectors** section.

The connector settings are displayed in the following columns of the table:

- **Name**

  Defined name of the connector.

- **Connector ID**

  ID assigned to the connector when it was created.

- **Enabled**

  Indicates whether the Server is ready for interaction with application modules of the connector. If this setting has a value of **No**, the Server does not accept requests from application modules of the connector.

- **Status**

  Operating status of application modules of the connector. The following statuses are available:

  - **Awaiting registration** – after adding an unmanageable connector or creating a new communication data package for the unmanageable connector, no connection has been established through this connector.
  - **Switchover** – the operating status of application modules of the connector is switched from a status of **Off** to **On**, or vice versa.
  - **Off** – the Server does not accept requests from application modules of the connector. If the connector is manageable, the command to stop running is sent to its application modules.
  - **On** – a successful connection was established through this connector using the certificate created for this connector.
  - **Error** – an error occurred when attempting to perform actions with the application modules of the connector.

- **Type**

  Icon and name of the connector type.

- **Last connection**

  Date and time of the last connection through this connector.

- **Manageable**

  Indicates that the connector is manageable. If this setting has a value of **No**, the connector is either unmanageable or is configured to ignore the functions of a manageable connector.

- **Changed**

  Date and time of the last modification of the connector settings.

- **Description**

  Defined description of the connector.

When viewing the connectors table, you can use the configuration, filter, search, and sorting functions.

Enabling and disabling a connector

If you want to temporarily prevent the application modules of a connector from connecting to the Server, you can disable this connector. To resume the connection, you will have to enable the connector.

To enable or disable a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the connector that you want to enable or disable.

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

4. Click **Enable** or **Disable** as relevant.

   A window with a confirmation prompt opens.

5. In the prompt window, click **OK**.

Editing connector settings

To edit connector settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the relevant connector.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. You can edit the settings the same as when you added the connector.

   Not all settings are available for editing. For example, the selected connector type cannot be changed.
6. Click **Save**.

The changes will be displayed in the corresponding columns of the connectors table. If you changed the connector name, the new name is displayed in the column header in the event types table.

When certain settings of an unmanageable connector are changed, the Server will generate a new communication data package for the connector (for example, this occurs if you change the server address for a **Syslog** connector that is configured to ignore the functions of a manageable connector). Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved communication data package. You will need to upload the contents of the new communication data package to the application that uses the connector. Otherwise, a new connection through the connector will be impossible for this application.

Creating a new communication data package for a connector

When an unmanageable connector is added, a communication data package is automatically created for this connector. If necessary, you can create a new communication data package for a connector (for example, if the certificate from the previous communication data package has been compromised and you had to update the certificate used for connecting connectors).

After a new communication data package is created, the certificate from the old communication data package becomes invalid. For this reason, you will have to use the new communication data package the next time you connect a recipient system through this connector.

To create a new communication data package for an unmanageable connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the unmanageable connector for which you want to create a new communication data package.

   The details area appears in the right part of the web interface window.
4. Click **Get new communication data package**.

   The **Generating a new communication data package** window opens.
5. Specify the settings for generating the communication data package:

   - User name that the recipient system will use to connect to the application through the connector. You must indicate the name of one of the application users.

     It is recommended to specify the user name that was indicated when adding the connector. If you need to specify the name of a different user, you are advised to select an application user account that was not indicated for other connectors and is not being used to connect to the Server through the web interface.
   - Address of the node where the connector application modules are running.
   - Password for accessing the connector certificate. Using the defined password, the certificate will be encrypted in the communication data package of the connector.
6. Click **Create communication data package**.

The Server generates a new communication data package for the selected connector, then the browser saves the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file. You will need to upload the contents of the obtained communication data package to the application that uses the connector. Otherwise, a new connection through the connector will be impossible for this application.

Deleting a connector

When a manageable connector is deleted, its application modules are automatically stopped and deleted from the connector deployment node.

Prior to deleting an unmanageable connector (or a connector that is configured to ignore the functions of a manageable connector), you first need to stop it manually and delete its application modules.

To prepare an unmanageable connector for deletion:

On the node where the connector is deployed, perform one of the following actions as appropriate:

- For a **Syslog**, **SIEM**, **Generic**, or **Email** connector, use the default_connectors_registrar.py script located in the directory /opt/kaspersky/kics4net-connectors/libexec/ on the node computer hosting the installed application components. To run the script, enter the following command in the operating system console:

  ```
  sudo python3 default_connectors_registrar.py delete
  ```

  After starting the script, specify the name of the connector when prompted by the script.

- For an **Active poll** connector, enter the following command in the operating system console:

  ```
  sudo systemctl disable kics4net-apm
  ```

To delete a connector:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Connectors**.
3. On the **Connectors** tab, select the connector that you want to delete.

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

   A window with a confirmation prompt opens.
5. In the prompt window, confirm removal of the selected connector.

Adding and deleting connector types

Connector types determine the available functional capabilities of connectors and the specific functionality that can be implemented within the scope of those capabilities. You can use the connector types that are already built into the application by Kaspersky and you can use additional connector types from other vendors.

To add a connector type to the application, you must obtain the following files from the vendor:

- Files for installing the application modules of connectors
- Connector type description file

If a connector type from a third-party vendor lets you save user account credentials in connectors for access to a recipient system, it is recommended to take measures to prevent these account credentials from being compromised. To minimize risks in case account credentials are compromised, it is recommended to provide only the minimum required permissions that these user accounts need for connections through the connectors.

The files for built-in connector types are included in the application distribution kit. These files are used to add connector types automatically during installation of application components. If built-in connector types are removed from the application for some reason, you can use the files from the distribution kit to re-add these connector types.

The connector types table is displayed under **Settings** → **Connectors** on the **Connector types** tab.

Viewing the connector types table

The connector types table is displayed under **Settings** → **Connectors** on the **Connector types** tab.

The connector settings are displayed in the following columns of the table:

- **Name**

  Connector type name defined by the vendor.

- **Vendor**

  Name of the connector type vendor.

- **Version**

  Connector type version number.

- **Code**

  Unique number of the connector type.

- **Capabilities**

  List of functional capabilities that will be available for connectors of this type.

When viewing the connector types table, you can use the configuration, filter, search, and sorting functions.

Adding a connector type

You can add a connector type to the application by using the description file provided by the vendor of this connector type. The description file of a connector type must be in a ZIP archive.

Installation of application modules for connectors of an added connector type must be performed manually using the files provided by the vendor of the connector type. Application modules need to be installed on the computers that will be specified as the connector deployment nodes when adding connectors.

To add a connector type:

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

2. Select **Settings** → **Connectors**.

3. On the **Connector types** tab, open the details by clicking **Add connector type**.

4. Click **Browse** to select the connector type description file.

5. Click **Save**.

   The new connector type will appear in the connectors table.

Deleting a connector type

When a connector type is deleted from the application, the application also deletes the information about this connector type as well as all connectors that were added using this connector type.

To delete a connector type:

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

2. Select **Settings** → **Connectors**.

3. On the **Connector types** tab, select the connector type that you want to delete.

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

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm removal of the selected connector type.

6. If the application has connectors of this type, also confirm removal of these connectors.

Managing security audit jobs

With Kaspersky Industrial CyberSecurity for Networks, you can conduct a security audit of the monitored devices. Security audit is performed by running the jobs created for the selected devices. Security audit jobs can be of the following types:

- Vulnerability and compliance audit.

  Vulnerability and compliance audit jobs let you assess device compliance with security standards and perform other checks (for example, search for vulnerabilities or detect installed software on devices).

- Configuration control.

  Configuration control jobs let you receive and save in the application detailed information about device configurations, as well as to use the application for comparing changes in device configurations.

- Active polling.

  Active polling jobs allow you to get the most accurate and complete information about the devices and their configurations directly from the devices themselves.

Users with any role except the Operator role can manage security audit jobs.

When using the security audit function, take into account the following special considerations and limitations:

- This functionality is available after a license key is added.
- Nodes that have the application components installed and are used for device scans within security audit jobs must have network access to devices to send and receive data. To provide network access to devices, the node computer must have a network interface providing a connection of these devices to the network. Network interfaces of monitoring points cannot be used for this purpose if these network interfaces receive mirrored industrial network traffic (for example, from SPAN ports of network switches).

Vulnerability and compliance audit jobs

You can use vulnerability and compliance audit jobs to conduct security audits of monitored devices. You can manually run security audit jobs or configure a schedule to automatically run each job.

When a job is started, the application initiates a scan of devices covered by this job. You can receive the job execution results by email or view and download the relevant data in the application web interface. Based on the job execution results and on the scans, the application can perform the following actions:

- Generate reports with information about the results.

  The application generates report files in PDF format. If sending reports by email is enabled in the job settings, the application automatically generates reports on each job execution and sends these reports to the specified recipients. If necessary, you can manually generate a report for a completed job or an individual device scan and then export the report to a file.

- Register detected risks of the Vulnerability category.

  For the risks registered based on the results of vulnerability and compliance audit jobs, the application indicates the source of the **OVAL** vulnerability. Such risks are registered by the application if registration of detected vulnerabilities is enabled in the job settings. At the same time, risks with the specified source of **OVAL** vulnerability are registered and processed irrespective of the risks for which other vulnerability sources are specified. Thus, the risk table may display risks with the same CVE ID (or an ID of a different vulnerability database), but with different vulnerability sources.

The vulnerability and compliance audit jobs must specify the rules used for conducting the audits. Rules can be written in the OVAL language or in the XCCDF language using OVAL definitions.

You can perform device scans as part of a job in one of the following device polling methods:

- **Local agent**

  You can use this method if the Endpoint Agent software component is installed on the devices selected for the job and integration between the EPP application and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Endpoint Agent on each device.

- **Remote connection**

  Use this method if the devices selected for the job do not have the Endpoint Agent software component installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. For this method, in the job settings specify one of the nodes with the installed application components from which connection to the devices is established. Also, specify the credentials for remote connections (credentials are stored in the application as secrets).

On devices running Linux operating systems, scans are performed using the commands to run standard diagnostic utilities for Linux devices.

You can manage vulnerability and compliance audit jobs on the **Vulnerability and compliance audit** tab in the **Security audit** section. If the **Remote connection** method is used to scan devices, you can create secrets with the necessary credentials under **Settings** → **Secrets**.

After the jobs are started and the device scans are completed, you can get information about the performed scans.

Adding a vulnerability and compliance audit job

For the existing sets of vulnerability and compliance audit rules, you can add jobs that the application uses to perform device scans.

Users with any role except the Operator role can add vulnerability and compliance audit jobs.

The vulnerability and compliance audit job is configured using the Wizard. The Wizard guides you step by step through the configuration of all required job settings. After the configuration is complete, you can wait for the scheduled scans to start on devices or start the scan job manually.

When adding a vulnerability and compliance audit job, you can invoke the Configuration Wizard in the following ways:

- Adding a job for a selected rule set. To do this:

  1. Select the **Security audit** section.
  2. On the **Rule sets** tab, select the rule set for which you want to add a vulnerability and compliance audit job.
  3. Click **Add job**.

  In the Configuration Wizard settings, the selected rule set is specified as default.

- Adding a job with blank settings. To do this:

  1. Select the **Security audit** section.
  2. On the **Vulnerability and compliance audit** tab, click **Add job**.

  The Configuration Wizard settings do not have the default values.

- Adding a job from an existing one. To do this:

  1. Select the **Security audit** section.
  2. On the **Vulnerability and compliance audit** tab, select the job based on which you want to add a new vulnerability and compliance audit job.
  3. Click **Copy**.

  The default values of the Configuration Wizard settings are set to the values of the existing job settings.

- Adding a job for selected devices. To do this:

  1. Select the **Assets** section.
  2. On the **Devices** tab, select the devices for which you want to add a vulnerability and compliance audit job.
  3. In the toolbar above the table of devices, open the **Create job** drop-down list and select **Vulnerability and compliance audit**.

  In the Configuration Wizard settings, a list of devices consisting of the selected devices is generated by default.

To configure job settings in the Configuration Wizard window:

1. In the **Select rules** section, do the following:

   a. Select the desired rule set for the job (not available when editing a job).

   b. Specify the profile of the selected rule set.

   c. Select the rules used to perform the scans and, if necessary, specify the desired values for the variables.

2. In the **Select devices** section, create a list of devices to run the scans during the job execution. Select up to 1,000 devices for the job.

   You can create a list of devices using the **Add to job** and **Delete from job** buttons. When you add devices, the application opens a window with a table of devices for selection. You can filter and sort the table to display the desired devices.

3. In the **Job configuration** section, configure the rest of the job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

   The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

   b. Select one of the following methods to poll devices:

   - **Local agent**

     You can use this method if the Endpoint Agent software component is installed on the devices selected for the job and integration between the EPP application and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Endpoint Agent on each device.

   - **Remote connection**

Use this method if the devices selected for the job do not have the Endpoint Agent software component installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. This method requires the following additional data:

- A node with the application components installed that will connect to the devices.
- Account credentials secret for remote connections

  You can select only one secret with one set of credentials for the job. The credentials stored in the selected secret must be valid on all devices selected for the job: connecting to these devices must be possible with the same credentials from the secret. Bear in mind that certain types of system data, such as passwords of operating system users, can be obtained only if requested by a user with a sufficiently high level of privileges. To get this data, you need to specify in the secret the credentials of a user with an appropriate level of privileges, such as a user with root access or a user listed in /etc/sudoers.

If a secret with the required credentials has not been added to the application, you can open a new tab in the browser without closing the Configuration Wizard window, connect to the Server and add the secret, and then use the button in the Configuration Wizard window to refresh the list of secrets.

c. If necessary, enable detection of risks of the Vulnerability category based on the job execution results. For this purpose, select the **Register detected vulnerabilities** check box.

d. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

- In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
- Depending on the selected option, specify the values for the settings to define the precise job start time.

The application runs the job according to the schedule, provided that the previous run of this job has been completed. If the previous run of this job still has the *Running* status when the scheduled job is supposed to start, the application skips the start of the scheduled job.

e. To send reports on the job starts by email, enable the **Send by email** option and specify the addresses of the recipients.

The maximum number of report recipients is 10.

4. Click **Create job** to close the wizard.

The specified settings are displayed in the job details, on the **Settings**, **Rules**, and **Devices** tabs.

Editing a vulnerability and compliance audit job

Users with any role except the Operator role can edit vulnerability and compliance audit jobs.

To edit a vulnerability and compliance audit job:

1. Select the **Security audit** section.
2. On the **Vulnerability and compliance audit** tab, select the job for which you want to change the settings.
3. Click **Edit**.

   The Configuration Wizard starts. The default values of the Configuration Wizard settings are set to the values of the selected job settings.
4. In the **Select devices** section, create a list of devices to run the scans during the job execution. Select up to 1000 devices for the job.

   You can create a list of devices using the **Add to job** and **Delete from job** buttons. When you add devices, the application opens a window with a table of devices for selection. You can filter and sort the table to display the desired devices.
5. In the **Job configuration** section, configure the rest of the job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

   The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

   b. Select one of the following methods to poll devices:

   - **Local agent**

     You can use this method if the Endpoint Agent software component is installed on the devices selected for the job and integration between the EPP application and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Endpoint Agent on each device.

   - **Remote connection**

     Use this method if the devices selected for the job do not have the Endpoint Agent software component installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. This method requires the following additional data:

     - A node with the application components installed that will connect to the devices.
     - Account credentials secret for remote connections

       You can select only one secret with one set of credentials for the job. The credentials stored in the selected secret must be valid on all devices selected for the job: connecting to these devices must be possible with the same credentials from the secret. Bear in mind that certain types of system data, such as passwords of operating system users, can be obtained only if requested by a user with a sufficiently high level of privileges. To get this data, you need to specify in the secret the credentials of a user with an appropriate level of privileges, such as a user with root access or a user listed in /etc/sudoers.

     If a secret with the required credentials has not been added to the application, you can open a new tab in the browser without closing the Configuration Wizard window, connect to the Server and add the secret, and then use the button in the Configuration Wizard window to refresh the list of secrets.

c. If necessary, enable detection of risks of the Vulnerability category based on the job execution results. For this purpose, select the **Register detected vulnerabilities** check box.

d. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

- In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
- Depending on the selected option, specify the values for the settings to define the precise job start time.

> The application runs the job according to the schedule, provided that the previous run of this job has been completed. If the previous run of this job still has the *Running* status when the scheduled job is supposed to start, the application skips the start of the scheduled job.

e. To send reports on the job starts by email, enable the **Send by email** option and specify the addresses of the recipients.

The maximum number of report recipients is 10.

6. Click **Save** to close the wizard.

The specified settings are displayed in the job details, on the **Settings**, **Rules**, and **Devices** tabs.

Viewing the table of vulnerability and compliance audit jobs

The vulnerability and compliance audit jobs table is displayed on the **Vulnerability and compliance audit** tab in the **Security audit** section.

The job settings are displayed in the following columns of the table:

- **Job ID**

  Job ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**

  Name used to represent the job in the application.

- **Description**

  Job description.

- **Created**

  Date and time when the job was added to the application.

- **Changed**

  Date and time when the job was last modified in the application.

- **Rule set**

  The name of the rule set associated with the job.

- **Profile**

  The name of the profile that defines the set of rules and variables for scans during the job execution.

- **XCCDF rules in set**

  The number of selected rules for the job and the total number of rules in the rule set.

- **Devices selected**

  The number of devices selected for the job.

- **Polling method**

  The polling method selected to scan devices: **Local agent** or **Remote connection**.

- **Register vulnerabilities**

  Flag indicating if detection of risks of the Vulnerability category is enabled based on the results of the job.

- **Schedule**

  Information about the schedule according to which the application automatically starts the job.

- **Status of last run**

  The resulting status of all device scans when the job was last run.

- **Last run**

  Date and time when the job was last started.

- **Next run**

  Date and time of the next scheduled start of the job.

When viewing the table of vulnerability and compliance audit jobs, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Manually starting and stopping vulnerability and compliance audit jobs

You can manually start and stop vulnerability and compliance audit jobs. When you start or stop a job, the application starts or stops all scans on the devices selected for this job.

You can stop or run the job depending on the status of the last job run. For example, a job cannot be started if the status of its last run is *Running*.

Users with any role except the Operator role can manually start and stop vulnerability and compliance audit jobs.

To start a vulnerability and compliance audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Vulnerability and compliance audit** tab, select the job you want to start.

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

4. Click **Run**. The button is disabled if the job cannot be started.

Kaspersky Industrial CyberSecurity for Networks starts the job. You can view information about the device scans in progress on the **Runs** tab in the job details.

To stop a vulnerability and compliance audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Vulnerability and compliance audit** tab, select the job you want to stop.

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

4. Click **Stop**. The button is disabled if the job cannot be stopped.

Viewing general information about the vulnerability and compliance audit job runs

You can view general information on the runs of vulnerability and compliance audit jobs in the jobs table. The table displays information about the most recent job runs not including the information about device scans. To view general information on all job runs, including information about the device scans, select the job and in the details area, open the **Runs** tab.

General information about vulnerability and compliance audit jobs runs includes the following:

- Job start status.

  The following statuses are available:

  - **New** or **Never run**: a new job run has been created, but no scans have been run yet.
  - **Pending**: a scan command is ready to be sent.
  - **Running**: the job is starting.
  - **Canceling**: the job start is being stopped.
  - **Canceled**: the job start has been stopped.
  - **Completed**: all scans have finished successfully.
  - **Error**: all scans have encountered an error.
  - **Partially successful** – the job completed with a partially successful result: some scans have the **Completed** status while some scans have a status of **Canceled** or **Error**.

- Device scan status.

The following statuses are available:

- **Pending**: a scan command is ready to be sent.
- **Running**: the scan is in progress.
- **Canceling**: the scan is being stopped.
- **Canceled**: the scan has been stopped.
- **Completed**: the scan has finished successfully.
- **Error**—an error occurred during the scan.

- Start date and time.
- End date and time.
- Execution duration.

Stopping a device scan in a vulnerability and compliance audit job

You can manually stop a device scan as part of the vulnerability and compliance audit job. When a device scan is stopped, the application does not stop other device scans within this job.

Users with any role except the Operator role can stop a device scan manually.

To stop a device scan within a vulnerability and compliance audit job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.
3. On the **Vulnerability and compliance audit** tab, select the job within which you want to stop a device scan.

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

4. In the details area, go to the **Runs** tab.
5. Select the desired scan and click **Stop** in the scan details area that appears. The button is disabled if the scan cannot be stopped.

Deleting vulnerability and compliance audit jobs

You can delete vulnerability and compliance audit jobs. However, you cannot delete the jobs with a last run status of **Running** or **Pending**.

Users with any role except the Operator role can delete vulnerability and compliance audit jobs.

To delete vulnerability and compliance audit jobs:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Vulnerability and compliance audit** tab, select the jobs you want to delete.

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm the deletion of the job.

   You can delete only the jobs whose last run status is not **Running** or **Pending**. If there are jobs with a status of **Running** or **Pending** among the selected jobs, the corresponding message is displayed. To delete such jobs, first stop the jobs.

Managing storage settings for the runs of vulnerability and compliance audit jobs

Kaspersky Industrial CyberSecurity for Networks saves information about the runs of vulnerability and compliance audit jobs in a database on the Server. Information about the job runs is stored until the jobs are deleted or until the specified limit is exceeded. If the amount of information about the job runs exceeds the specified limit, the application automatically deletes 10% of the oldest records. If the minimum storage time limit is enabled and the application deletes entries whose storage time is less than the defined limit, a corresponding message will appear in the application message log. You can configure the settings for storing information about the job runs.

To change the storage settings for the runs of vulnerability and compliance audit jobs:

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

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

3. Select the Server tile.

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

4. Click **Edit**.

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

5. On the **General** tab, go to the **Vulnerability and compliance audit** section and use the **Max volume** setting to define the size limit for storing information about job runs.

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

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.

6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for information about job runs, and specify the minimum number of days.

7. Click **Save**.

Configuration control jobs

Using the configuration control jobs, you can conduct a security audit of monitored devices in terms of receiving, saving, and comparing device configurations. Configuration control jobs additionally let you upload data to Kaspersky Industrial CyberSecurity for Networks for device user control, device application and patch monitoring, and OT device hardware monitoring.

The application can monitor the following device types:

- **Windows operating system** – includes configurations of devices with Windows operating systems.
- **Linux operating system** – includes configurations of devices with Linux operating systems.
- **Network devices**—includes configurations of devices categorized as network equipment (for example, routers and switches).
- **PLC**—includes configurations of programmable logic controllers or any other devices whose configurations can be received using connectors of the **Active poll** type.

For details on data retrieval depending on the selected device type, see the Appendix.

You can manually run security audit jobs or configure a schedule to automatically run each job.

When a job is started, the application initiates a scan of devices covered by this job. If a device scan detects configuration changes for the device, the application registers an event. Depending on the configuration processing mode selected for the job, the event contains the comparison results of the received configuration with the previous configuration of the device or with its golden configuration.

The following configuration processing modes are provided for configuration control jobs:

- **Update only** – only the last received configuration is saved for each device.
- **Archive versions** – all unique configurations are saved for each device.
- **Compare to golden configuration** – all unique configurations are saved for each device, while the newly received configuration is compared with the golden configuration (by default, this is the first loaded device configuration).

You can scan devices to get configurations for the **PLC** device type only if you use **Active Poll** connectors. The following device polling methods are provided for getting the remaining device types:

- **Local agent**

  You can use this method if the Endpoint Agent software component is installed on the devices selected for the job and integration between the EPP application and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Endpoint Agent on each device.

- **Remote connection**

  Use this method if the devices selected for the job do not have the Endpoint Agent software component installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. The method is supported for getting configurations for the **Linux operating system** and **Network devices** device types. For this method, in the job settings specify one of the nodes with the installed application components from which connection to the devices is established. Also, specify the credentials for remote connections (credentials are stored in the application as secrets).

You can manage configuration control jobs on the **Configuration control** tab in the **Security audit** section. If the **Active poll** connector or the **Remote connection** method is used to scan devices, you can create secrets with the necessary credentials under **Settings** → **Secrets**.

After the jobs are run and the device scans are completed, you can view information about the received device configurations in the device details area on the **Configurations** tab. The options for comparing configurations and assigning a golden configuration are also available on this tab.

You can view information about registered events when connected to the Server through the web interface.

Adding a configuration control job

For devices known to the application, you can add jobs to receive, save, and compare device configurations.

Users with any role except the Operator role can add configuration control jobs.

The configuration control job is configured using the Wizard. The Wizard guides you step by step through the configuration of all required job settings. After the configuration is complete, you can wait for the scheduled scans to start on devices or start the scan job manually.

When adding a configuration control job, you can invoke the Configuration Wizard in the following ways:

- Adding a job with blank settings. To do this:

  1. Select the **Security audit** section.
  2. On the **Configuration control** tab, click **Add job**.

  The Configuration Wizard settings do not have the default values.

- Adding a job for selected devices. To do this:

  1. Select the **Assets** section.
  2. On the **Devices** tab, select the devices for which you want to add a configuration control job.
  3. You can select no more than 100 devices.
  4. In the toolbar above the table of devices, open the **Create job** drop-down list and select **Configuration control**.

  In the Configuration Wizard settings, a list of devices consisting of the selected devices is generated by default.

To configure job settings in the Configuration Wizard window:

1. In the **Select devices** section, create a list of devices to run the scans during the job execution. Select up to 100 devices for the job.

   You can create a list of devices using the **Add to job** and **Delete from job** buttons. When you add devices, the application opens a window with a table of devices for selection. You can filter and sort the table to display the desired devices.

2. In the **Select settings** section, do the following:

   a. Select the device type to receive when the job is being executed.

   b. If you have chosen the **PLC** device type, read the active polling considerations when a warning window appears, and confirm that you accept the risks associated with using the active polling module.

   c. Configure the settings of the selected device type. Depending on the selected type, you can specify the required configuration types (such as **Users**) or specify the connection details (such as a connector and an account credentials secret for remote connections if the **PLC** device type is selected.

      If a secret with the required credentials has not been added to the application, you can open a new tab in the browser without closing the Configuration Wizard window, connect to the Server and add the secret, and then use the button in the Configuration Wizard window to refresh the list of secrets.

3. In the **Job configuration** section, configure the rest of the job settings:

   a. Enter the job name and description.

      You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

      The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

   b. Select configuration processing mode.

   c. If the **Select settings**, **Windows operating system**, or **Linux operating system** device type is selected in the **Network devices** section, select one of the following methods to poll devices:

      - **Local agent**

        You can use this method if the Endpoint Agent software component is installed on the devices selected for the job and integration between the EPP application and Kaspersky Industrial CyberSecurity for Networks is configured. This method is used for scanning using Endpoint Agent on each device.

      - **Remote connection**

        Use this method if the devices selected for the job do not have the Endpoint Agent software component installed, but it is possible to connect to these devices via protocols that ensure secure management and data transfer. The method is supported for getting configurations for the **Linux operating system** and **Network devices** device types. This method requires the following additional data:

        - A node with the application components installed that will connect to the devices.

        - Account credentials secret for remote connections

          You can select only one secret with one set of credentials for the job. The credentials stored in the selected secret must be valid on all devices selected for the job: connecting to these devices must be possible with the same credentials from the secret. Bear in mind that certain types of system data, such as passwords of operating system users, can be obtained only if requested by a user with a sufficiently high level of privileges. To get this data, you need to specify in the secret the credentials of a user with an appropriate level of privileges, such as a user with root access or a user listed in /etc/sudoers.

If a secret with the required credentials has not been added to the application, you can open a new tab in the browser without closing the Configuration Wizard window, connect to the Server and add the secret, and then use the button in the Configuration Wizard window to refresh the list of secrets.

d. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

- In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
- Depending on the selected option, specify the values for the settings to define the precise job start time.

The application runs the job according to the schedule, provided that the previous run of this job has been completed. If the previous run of this job still has the *Running* status when the scheduled job is supposed to start, the application skips the start of the scheduled job.

4. Click **Create job** to close the wizard.

The specified settings are displayed in the job details, on the **Settings** and **Devices** tabs.

Editing a configuration control job

Users with any role except the Operator role can edit a configuration control job.

To edit a configuration control job:

1. Select the **Security audit** section.
2. On the **Configuration control** tab, select the job for which you want to change the settings.
3. Click **Edit**.

   The Configuration Wizard starts. The default values of the Configuration Wizard settings are set to the values of the selected job settings.
4. In the **Job configuration** section, configure the job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

   The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

   b. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

   - In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   - Depending on the selected option, specify the values for the settings to define the precise job start time.

The application runs the job according to the schedule, provided that the previous run of this job has been completed. If the previous run of this job still has the *Running* status when the scheduled job is supposed to start, the application skips the start of the scheduled job.

5. Click **Save** to close the wizard.

The specified settings are displayed in the job details, on the **Settings** and **Devices** tabs.

Viewing the table of configuration control jobs

The configuration control jobs table is displayed on the **Configuration control** tab in the **Security audit** section.

The job settings are displayed in the following columns of the table:

- **Job ID**

  Job ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**

  Name used to represent the job in the application.

- **Description**

  Job description.

- **Created**

  Date and time when the job was added to the application.

- **Changed**

  Date and time when the job was last modified in the application.

- **Device type**

  The name of the device type selected for the job.

- **Devices selected**

  The number of devices selected for the job.

- **Polling method**

  The polling method selected for device scanning: **Local agent**, **Remote connection**, or **Active poll connector**.

- **Schedule**

  Information about the schedule according to which the application automatically starts the job.

- **Status of last run**

  The resulting status of all device scans when the job was last run.

- **Last run**

  Date and time when the job was last started.

- **Next run**

  Date and time of the next scheduled start of the job.

When viewing the table of configuration control jobs, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Manually starting and stopping configuration control jobs

You can manually start and stop configuration control jobs. When you start or stop a job, the application starts or stops all scans on the devices selected for this job.

You can stop or run the job depending on the status of the last job run. For example, a job cannot be started if the status of its last run is *Running*.

Users with any role except the Operator role can manually start and stop configuration control jobs.

To start a configuration control job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Configuration control** tab, select the job you want to start.

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

4. Click **Run**. The button is disabled if the job cannot be started.

Kaspersky Industrial CyberSecurity for Networks starts the job. You can view information about the device scans in progress on the **Runs** tab in the job details.

To stop a configuration control job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Configuration control** tab, select the job you want to stop.

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

4. Click **Stop**. The button is disabled if the job cannot be stopped.

Viewing general information about the configuration control job runs

You can view general information on the runs of configuration control jobs in the jobs table. The table displays information about the most recent job runs not including the information about device scans. To view general information on all job runs, including information about the device scans, select the job and in the details area, open the **Runs** tab.

General information about configuration control job runs includes the following:

- Job start status.

  The following statuses are available:

  - **New** or **Never run**: a new job run has been created, but no scans have been run yet.
  - **Pending**: a scan command is ready to be sent.
  - **Running**: the job is starting.
  - **Canceling**: the job start is being stopped.
  - **Canceled**: the job start has been stopped.
  - **Completed**: all scans have finished successfully.
  - **Error**: all scans have encountered an error.
  - **Partially successful** – the job completed with a partially successful result: some scans have the **Completed** status while some scans have a status of **Canceled** or **Error**.

- Device scan status.

  The following statuses are available:

  - **Pending**: a scan command is ready to be sent.
  - **Running**: the scan is in progress.
  - **Canceling**: the scan is being stopped.
  - **Canceled**: the scan has been stopped.
  - **Completed**: the scan has finished successfully.
  - **Error**—an error occurred during the scan.

- Start date and time.
- End date and time.
- Execution duration.

Assigning a golden device configuration

The application stores captured configurations for each device while running configuration control jobs. If configuration processing mode is set to **Compare to golden configuration**, the application considers the first loaded device configuration as golden. You can set any other saved device configuration as golden.

If necessary, you can compare saved device configurations before assigning a golden configuration.

To set a golden device configuration:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Devices** tab in the **Assets** section, select the relevant device.

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

3. On the **Configurations** tab, in the details area, select the table row with the desired configuration type, such as **Users**, which stores user data. The selected type must have a value of at least 2 in the **Total configurations** column.

   You will see a window containing detailed information about the selected configuration type.

4. In the drop-down list, select the date and time when the configuration you want to set as the golden configuration was received.

   The window will display detailed information about the saved configuration of the selected type.

5. Click **Set as golden configuration**.

6. In the prompt window, confirm the assignment of the golden configuration.

Stopping a device scan in a configuration control job

You can manually stop a device scan as part of the configuration control job. When a device scan is stopped, the application does not stop other device scans within this job.

Users with any role except the Operator role can stop a device scan manually.

To stop a device scan within a configuration control job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Configuration control** tab, select the job within which you want to stop a device scan.

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

4. In the details area, go to the **Runs** tab.

5. Select the desired scan and click **Stop** in the scan details area that appears. The button is disabled if the scan cannot be stopped.

Deleting configuration control jobs

You can delete configuration control jobs. However, you cannot delete the jobs with a last run status of **Running** or **Pending**.

Users with any role except the Operator role can delete configuration control jobs.

To delete configuration control jobs:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Configuration control** tab, select the jobs you want to delete.

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm the deletion of the job.

   You can delete only the jobs whose last run status is not **Running** or **Pending**. If there are jobs with a status of **Running** or **Pending** among the selected jobs, the corresponding message is displayed. To delete such jobs, first stop the jobs.

Active device polling jobs

Using the active polling jobs, you can conduct a security audit of monitored devices in terms of receiving accurate and complete information about devices and their configurations directly from the devices themselves. Active polls are performed by using connectors. To conduct active polling of devices, one or more **Active poll** connectors must be added to the application.

Connectors provide various methods for conducting active polling. The available *active polling methods* depend on the utilized protocols and the commands and functions of these protocols. The application's built-in **Active poll** connector type contains a set of methods supporting active polls over application-layer protocols and common protocols. Kaspersky Industrial CyberSecurity for Networks supports the following methods to actively poll the devices:

- Polling via ARP (only for computers with the kernel version 4.3 or later)
- Polling via DNP3
- Getting process control settings and tags (only for computers with the kernel version 4.3 or later)
- Polling via IEC 61850: MMS
- Polling via Modbus TCP
- Polling via BECKHOFF ADS/AMS over UDP
- Polling via PROFINET DCP (only for computers with the kernel version 4.3 or later)
- Polling via Siemens S7comm over Industrial Ethernet
- Polling via Siemens S7comm over TCP
- Getting extended configuration of Schneider Electric Modicon M340/M580

- Getting Siemens SIMATIC S7-300/S7-400 extended configuration
- Obtaining Emerson DeltaV extended configuration
- Obtaining Rockwell Automation Allen-Bradley extended configuration
- Polling via SMB
- Polling via SNMP
- Polling via SSH
- Polling via WinRM HTTP
- Polling via WinRM HTTPS
- Polling via WMI
- Risk analysis on Cisco devices via SSH
- Risk analysis on Linux devices via SSH

The methods are distinguished by the specific device information that they obtain. You can select the relevant information you need and the methods you want to use when configuring the active polling settings.

Some methods use secrets to connect to devices. Device connections are made using credentials from secrets added to the application.

When using these methods, the application can automatically update the following device information based on the active polling results:

- Name used to represent a device in the application.
- Name used to represent the device in the network (network name).
- Name of the device hardware vendor.
- Device model name.
- Device hardware version number.
- Name of the device software vendor.
- Device software name.
- Device software version number.
- Address information for network interfaces of the device.
- Name of the operating system installed on the device (only for devices running Windows and Linux operating systems).
- Configuration of Process Control settings and tags.
- Advanced configuration for industrial devices.

The list of operating systems supported by the application for active polling of devices is provided in the Appendix.

Data for which automatic updates are disabled (is displayed) does not update automatically whenever a device is added or device details are changed. The application also evaluates the authenticity of received device information and in some cases may reject unreliable updates of previously received information.

Some active polling methods support the capability to detect risks and to make changes to the topology map based on obtained device information.

You can manually run security audit jobs or configure a schedule to automatically run each job. Users with any role except the Operator role can run the device active device polling jobs.

To utilize active polling functionality, you need to take into account the following special considerations and limitations:

- This functionality is available after a license key is added.
- Application modules of the connectors used to conduct active polling of devices must have network access to the devices so that they can send requests and receive data from the devices. If application modules are running on a node that has application components installed, to ensure network access to devices this computer must have a network interface with a connection to the network of these devices. Network interfaces of monitoring points cannot be used for this purpose if these network interfaces receive mirrored industrial network traffic (for example, from SPAN ports of network switches).
- Active polling may result in some unforeseen issues with devices due to the possibility that these devices may incorrectly interpret the incoming active polling commands. These issues may be caused by an inappropriate or highly specialized configuration of devices. Issues may also arise due to latent errors in the network configuration that are not apparent during normal interactions between the devices. Consequently, active polling poses the following risks of potential impact on devices:
  - Device shutdown
  - Loss of connectivity with the device
  - Complete or partial device malfunction
  - Slower-than-normal operation
  - Other potential malfunctions in the network and equipment

Adding active polling job

For devices known to the application, you can add active polling jobs.

Users with any role except the Operator role can add active polling jobs. Adding active polling jobs is available after adding a license key.

The active polling job is configured using the Wizard. The Wizard guides you step by step through the configuration of all required job settings. After the configuration is complete, you can wait for the scheduled scans to start on devices or start the scan job manually.

When adding an active polling job, you can invoke the Configuration Wizard in the following ways:

- Adding a job with blank settings. To do this:

  1. Select the **Security audit** section.
  2. On the **Active polling** tab, click **Add job**.

  The Configuration Wizard settings do not have the default values.

- Adding a job for selected devices. To do this:

  1. Select the **Assets** section.
  2. On the **Devices** tab, select the devices for which you want to add an active polling job. You can select no more than 100 devices.
  3. In the toolbar above the table of devices, open the **Create job** drop-down list and select **Active polling**.

  In the Configuration Wizard settings, a list of devices consisting of the selected devices is generated by default.

To configure job settings in the Configuration Wizard window:

1. Read the active polling considerations in the warning window, and confirm that you accept the risks associated with using the active polling module.
2. In the **Select devices** section of the wizard, create a list of devices for which you want to perform active polling. Select up to 100 devices.

   You can create a list of devices using the **Add to job** and **Delete from job** buttons. When you add devices, the application opens a window with a table of devices for selection. You can filter and sort the table to display the desired devices.
3. In the **Select settings** section of the wizard, select the check boxes for the specific device information that you want to update using active polling. You can also enable risk detection (the **Risks** check box) and discovery of topology settings for devices (the **Topology settings** check box).
4. In the **Select methods** section of the wizard, do the following:

   a. Select an active polling module.

   b. Select the check boxes for the specific methods that you want to use for getting device information, risk detection, and/or reading topology settings.

   The available methods are grouped based on the connectors that provide the capabilities for active polling of devices. The list contains only the methods that are capable of obtaining the selected information. If a connector cannot be used for active polling of selected devices, available methods are not displayed for this connector (for example, if the connector is disabled or if an address space not containing addresses of selected devices is selected for the connector).

   c. Configure the methods for each connector as needed. For example, for **Polling via SSH**, specify a port and a credentials secret.

If a secret with the required credentials has not been added to the application, you can open a new tab in the browser without closing the Configuration Wizard window, connect to the Server and add the secret, and then use the button in the Configuration Wizard window to refresh the list of secrets.

Methods that require configuring settings are highlighted in red. To update the settings, click the button to the right of the desired method.

5. In the **Job configuration** section of the wizard, configure the rest of the job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

   The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

   b. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

   - In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
   - Depending on the selected option, specify the values for the settings to define the precise job start time.

   The application runs the job according to the schedule, provided that the previous run of this job has been completed. If by the time a scheduled job is started its previous launch has the *Running* status, the application skips the start of the scheduled job.

6. Click **Create job** or **Create and run** to close the wizard.

The specified settings are displayed in the job details.

Editing an active polling job

Users with any role except the Operator role can edit active polling jobs.

To edit an active polling job:

1. Select the **Security audit** section.
2. On the **Active polling** tab, select the job for which you want to change the settings.
3. Click **Edit**.

   The Configuration Wizard starts. The default values of the Configuration Wizard settings are set to the values of the selected job settings.

4. In the **Job configuration** section of the wizard, configure the rest of the job settings:

   a. Enter the job name and description.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The job name must begin and end with any permitted character except space.

The job name must contain no more than 256 characters. The job description must contain no more than 4096 characters.

b. To run the job according to a schedule, enable the **Run job according to schedule** option and configure the schedule settings:

- In the **Frequency** drop-down list, select how often to run the job: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
- Depending on the selected option, specify the values for the settings to define the precise job start time.

The application runs the job according to the schedule, provided that the previous run of this job has been completed. If the previous run of this job still has the *Running* status when the scheduled job is supposed to start, the application skips the start of the scheduled job.

5. Click **Save** to close the wizard.

The specified settings are displayed in the job details.

Viewing the table of active polling jobs

The active polling jobs table is displayed on the **Active polling** tab in the **Security audit** section.

The job settings are displayed in the following columns of the table:

- **Job ID**

  Job ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**

  Name used to represent the job in the application.

- **Description**

  Job description.

- **Created**

  Date and time when the job was added to the application.

- **Changed**

  Date and time of the last modification in the application.

- **Devices selected**

  The number of devices selected for the job.

- **Schedule**

  Information about the schedule according to which the application automatically starts the job.

- **Status of last run**

  The resulting status of all device scans when the job was last run.

- **Last run**

  Date and time when the job was last started.

- **Next run**

  Date and time of the next scheduled start of the job.

When viewing the table of active polling jobs, you can use the configuration, filter, search, and sorting functions.

Starting and stopping active polling jobs

You can manually start and stop active polling jobs. When you start or stop a job, the application starts or stops all scans on the devices selected for this job.

You can stop or run the job depending on the status of the last job run. For example, a job cannot be started if the status of its last run is *Running*.

Users with any role except the Operator role can manually start and stop active polling jobs.

To start an active polling job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Active polling** tab, select the job you want to start.

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

4. Click **Run**. The button is disabled if the job cannot be started.

   Kaspersky Industrial CyberSecurity for Networks starts the job. You can view information about the device scans in progress on the **Runs** tab in the job details.

To stop an active polling job:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Security audit** section.

3. On the **Active polling** tab, select the job you want to stop.

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

4. Click **Stop**. The button is disabled if the job cannot be stopped.

Viewing general information about the active polling job runs

You can view general information on the runs of active polling jobs in the jobs table. The table displays information about the most recent runs not including the information about device scans. To view general information on all job runs, including information about the device scans, select the job and in the details area, open the **Runs** tab.

General information about active polling job runs includes the following:

- The job status or the device scan status.

  The following statuses are available:

  - **Pending** – a command to start the scan has not been sent yet.
  - **Running** – the job is starting, or the scan is in progress.
  - **Canceling** – the start of the job or scanning is being stopped.
  - **Canceled** – the start of the job or scanning is stopped.
  - **Completed** – the scan completed successfully or all scans within the job run completed successfully.
  - **Error** – an error occurred during a scan or errors occurred in all scans within the job run.
  - **Partially successful** – the job completed with a partially successful result: some scans have the **Completed** status while some scans have a status of **Canceled** or **Error**.
- Start date and time.
- End date and time.
- Execution duration.

Viewing a report on the active polling job execution

You can view reports containing the device scan results when viewing the details of an active polling job run. The application generates reports for the jobs completed with the following statuses: **Completed**, **Partially successful**, **Canceled**, and **Error**.

In the report, the following details are displayed:

- Name of the device that was scanned.
- Device settings update status.
- List of device settings grouped by their update status.
- List of methods grouped by their execution status. If an error occurs when a method is being employed, the application displays its reason.

To view a report on the active polling job execution:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select the **Security audit** section.
3. On the **Active polling** tab, select the job for which you want to view the run report.

   The details area appears in the right part of the web interface window.
4. In the details area, go to the **Runs** tab and select the desired job run.

   The details area appears in the right part of the web interface window. The details area displays detailed information about the selected job run.

Deleting active polling jobs

You can delete active polling jobs. However, you cannot delete the jobs with a last run status of **Running** or **Pending**.

Users with any role except the Operator role can delete active polling jobs.

To delete active polling jobs:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.
2. Select the **Security audit** section.
3. On the **Active polling** tab, select the jobs you want to delete.
4. Click **Delete**.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm the deletion of the job.

   You can delete only the jobs whose last run status is not **Running** or **Pending**. If there are jobs with a status of **Running** or **Pending** among the selected jobs, the corresponding message is displayed. To delete such jobs, first stop the jobs.

Forming a topology map

A topology map is a visual representation of the physical connections between devices in the industrial network. In contrast to the network interaction map, the topology map is intended for displaying the actual connections between devices via network cables connected to the ports of network interfaces. After generating a topology map, you will see one or more graphs that visually display the structure of connections between devices via network equipment such as switches, hubs, routers, and others.

The following objects may be displayed on the topology map:

- Nodes. These objects represent devices and network equipment.
- Links. These objects represent the physical connections between nodes.

Nodes are constantly displayed on the topology map regardless of whether or not these nodes have connections to other nodes. Nodes can be filtered for a more convenient display. Nodes are also distinguished in various ways on the topology map depending on their types, statuses, and events related to the nodes.

After links are added for nodes, you can arrange these nodes on the topology map according to a topology generation procedure.

The topology map is displayed on the **Topology map** tab in the **Network map** section.

Data for adding connections to the topology map can be obtained automatically based on the results of active polling of devices – if the corresponding polling methods are used (for example, polling via SNMP). You can also add connections manually.

Nodes on the topology map

Nodes on the topology map can be of the following types:

- A device that is known to the application. This type of node represents a device that is listed in the table of devices.
- Unmanaged switch. This type of node represents a device whose MAC- and IP addresses are either unavailable or unknown. Due to its lack of address information, this device cannot be added to the table of devices. However, such a device can still be linked to other devices. For instance, this type of node may appear on the topology map if active polling detects multiple connections of different devices to one port of the same device. If this is the case, the application determines that an unidentified switching device (such as a hub) is present in the network, and automatically creates a node for this device. No more than 1000 unmanaged switches can be added to the application.

  If you are able to identify the MAC- and/or IP address of a node for an unmanaged switch, you can use this unmanaged switch node to manually add a new device to the table of devices.

Displayed information on nodes representing devices

The following information is displayed for nodes representing known devices when the topology map scale is maximized:

- Assigned device name.
- Device category icon.
- Network name or address of the device (if an IP address is not assigned, the MAC address is displayed).

- Various icons depending on fulfillment of the following conditions:
  - If the router indicator has been set for the device.
  - If an EPP application is installed on the device (the color of the icon depends on the connection status).
  - If the device has a status of *Archived*.
- The thick line on the left border of a node has one of the following colors depending on the device's security state:
  - Green signifies the *OK* security state.
  - Yellow signifies the *Warning* security state.
  - Red signifies the *Critical* security state.

If a device has a status of *Unauthorized*, the node has a red background.

Displayed information on nodes representing unmanaged switches

The following information is displayed for the nodes representing unmanaged switches when the topology map scale is maximized:

- Defined node name.
- Unmanaged switch icon.

Nodes representing unmanaged switches have a gray background.

Links on the topology map

Links on the topology map show the physical connections between nodes. Each link represents a connection between ports of network interfaces on devices connected via network cable.

Links are displayed as horizontal or vertical lines on the topology map. Multiple link lines extending from one node on shared sections of the map are displayed as a thick line representing a network bus.

Viewing details about objects on the topology map

Detailed information about objects presented on the topology map is displayed in the details area. To display details, you can select an object by clicking it.

The following information is displayed for the selected node:

- If a node represents a known device, the details area displays the same information that is displayed when selecting a device in the table of devices.
- If a node represents an unmanaged switch, the details area displays the following information:
  - Name of the unmanaged switch node
  - Type of node (Unmanaged switch)
  - **Topology settings** section containing a list of ports for which links with other nodes were added or may be added

Name of one of the link nodes and list of ports of this node with connections to other nodes is displayed for the selected connection. If a bus is selected, you will see a list of ports of the node that has the highest number of links in the selected bus.

Adding nodes to the topology map

When generating a topology map, the application can automatically add detected nodes to the topology map. If some relevant nodes were not automatically added by the application, you can manually add them when working with the topology map.

Users with any role except the Operator role can add nodes manually.

If you know the MAC- and/or IP address of a device that you want to add to the topology map as a node, you can manually add this device. If the address information of a node is unknown or missing (for example, if the device is a hub), you can add an unmanaged switch node.

To add an unmanaged switch to the topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, select **New unmanaged switch** in the **Add node** drop-down list.

   A details area with the unmanaged switch settings appears in the right part of the window.

3. Enter the node name.

   The node name must be unique (must not match the names of other unmanaged switches) and must contain no more than 100 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. The node name must begin and end with any permitted character except a space.

4. Click **Save**.

The unmanaged switch node will appear on the topology map. Then you will be able to add links with this node for other nodes.

Manually adding links to the topology map

This section provides instructions on adding links to the topology map. You can manually add links and configure their settings when working with the table of devices or topology map.

Users with any role except the Operator role can add connections and configure their settings.

Adding links for a selected node and configuring additional topology settings

This function is convenient if you want to add multiple links with other nodes for one node (for example, add all links for a switch). When using this method for adding links, you can also configure all topology settings for the device.

To add links for a node and configure additional topology settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the node on the **Topology map** tab in the **Network map** section.

   You can also select the device represented by the relevant node on the **Network interaction map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select an unmanaged switch node.

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

3. In the upper right corner of the details area, click the ⋮ icon and select **Topology settings** → **Configure settings**.

   The window for configuring the ports and connections of the selected node is displayed.

4. In the **Physical ports** settings group, add information about links with other nodes. Information about each link must be provided in a separate line in which you can specify the following settings:

   - Name of the physical port where the network cable is connected (optional setting)
   - VLAN IDs (optional setting)
   - Addresses of the network interface connected to the port (optional setting)
   - Node that will serve as the second side of the connection (to select a node, you will see a window containing the table of available nodes and ports on nodes)

5. If necessary, provide information on the virtual ports of the device in the **Virtual ports** settings group.

   Information on virtual ports is not used for generating the topology map.

6. Click **Save**.

Adding links for selected nodes without configuring additional topology settings

This function is convenient if you want to add links of multiple nodes with one node (for example, add a link with one switch for each of the selected nodes). When using this method for adding links, the additional settings of these links will remain undefined. For instance, you cannot select a port on the node for connections to be added. You can configure the additional settings of links after they are added when editing the topology settings for a node.

Links can be added if no more than 50 rules are selected.

To add links for nodes without configuring additional settings of links:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select one or more nodes on the **Topology map** tab in the **Network map** section.

   To select multiple nodes, perform one of the following actions:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

   You can also select devices represented by the relevant nodes on the **Network interaction map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select nodes of unmanaged switches.

3. Right-click to open the context menu.

4. In the context menu, select **Add connection with node**.

   You will see a window containing a table of nodes available for selection.

5. Select the relevant node in the table and click **OK**.

Editing the topology settings for a node

When editing topology settings, you can add, configure, and delete links for a node, and configure settings of the virtual nodes.

Users with any role except the Operator role can edit the topology settings.

To configure the topology settings for a node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the node on the **Topology map** tab in the **Network map** section.

You can also select the device represented by the relevant node on the **Network interaction map** tab or on the **Devices** tab in the **Assets** section. However, on these tabs you will not be able to select an unmanaged switch node.

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

3. In the upper right corner of the details area, click the ⋮ icon and select **Topology settings** → **Configure settings**.

   The window for configuring the ports and connections of the selected node is displayed.

4. In the **Physical ports** settings group, provide information about links with other nodes. Information about each link must be provided in a separate line in which you can specify the following settings:

   - Name of the physical port where the network cable is connected (optional setting)
   - VLAN IDs (optional setting)
   - Addresses of the network interface connected to the port (optional setting)
   - Node that will serve as the second side of the connection (to select a node, you will see a window containing the table of available nodes and ports on nodes)

5. If necessary, provide information on the virtual ports of the device in the **Virtual ports** settings group.

   Information on virtual ports is not used for generating the topology map.

6. Click **Save**.

Renaming the node of an unmanaged switch

You can rename an unmanaged switch node added to the topology map either automatically or manually.

Users with any role except the Operator role can rename an unmanaged switch node.

To rename an unmanaged switch node on the topology map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, select the unmanaged switch node.

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

3. Click **Edit**.

4. In the field containing the current name of the node, enter a new name.

   The node name must be unique (must not match the names of other unmanaged switches) and must contain no more than 100 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ ' , . - _ = +`. The node name must begin and end with any permitted character except a space.

5. Click **Save**.

Deleting objects from the topology map

You can delete nodes and connections when working with a topology map. When nodes representing known devices are deleted, the devices are deleted from the table of devices.

Users with any role except the Operator role can delete objects from the topology map.

To delete a node:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, select the node you want to delete.

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

3. Click **Delete**.

   A window with a confirmation prompt opens.

4. In the prompt window, confirm removal of the selected node.

To delete a link or bus (multiple links):

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. On the **Topology map** tab in the **Network map** section, select the link or bus.

3. Click **Delete**.

   A window with a confirmation prompt opens.

4. In the prompt window, confirm removal of the selected links.

Changing the topology map scale

The topology map can be displayed in a scale of 1–100%. The current scale value is displayed in the toolbar located in the left part of the topology map display area.

To change the scale of the topology map:

Use the mouse wheel or the **+** and **–** buttons located in the toolbar next to the current scale value.

Reducing the scale of the map reduces the amount of information that is displayed in nodes.

If the display scale is less than 25%, icons and text information are not displayed in nodes. With this reduced scale, on each node representing a known device, the upper-right corner displays the device status as a triangle in one of the following colors:

- Green signifies that the device has a status of *Authorized*.
- Red signifies that the device has a status of *Unauthorized*.
- Gray signifies that the device has a status of *Archived*.

Positioning of the topology map

If necessary, you can change the positioning of the topology map either manually or automatically. Automatic positioning lets you move the map and change its scale in such a way to display all nodes that satisfy the defined filter settings.

To manually position the topology map:

1. Position the mouse cursor over any part of the topology map that is not occupied by objects.
2. Click and hold the left mouse button to drag the topology map image.

To automatically position the topology map:

Click the button in the toolbar located in the left part of the topology map display area.

The positioning and scale of the map will change to display all nodes.

Pinning and unpinning nodes on the topology map

By default, nodes are not pinned on the network map. Unpinned nodes may be automatically arranged for optimal display of other objects.

Nodes are pinned when their location is changed manually. You can also pin the current location of displayed objects without moving them.

To pin and unpin objects without moving them, you can use the buttons in the toolbar located in the left part of the topology map display area. You can use the and buttons to pin and unpin all nodes displayed on the topology map. The buttons are available if the topology map contains objects for which the corresponding actions can be applied.

After the location of a node is pinned, the icon appears in the upper-right corner of this element (if the topology map has a scale of less than 25%). You can also use this icon to unpin the object.

The location of a pinned node is retained. If a pinned node disappears from the topology map (for example, after a filter is applied), this node will be displayed in the same location the next time it appears (or nearby, if this place is already occupied by another pinned node).

Manually changing the location of nodes on the topology map

You can manually change the location of nodes on the topology map by using the arrangement method that is most convenient for you.

After their arrangement, nodes are pinned in their new location. If necessary, you can unpin these objects.

To change the position of nodes on the topology map:

1. On the topology map, select one or multiple nodes.

   To select multiple nodes, perform one of the following actions:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

2. Use your mouse to drag the selected objects to the necessary location.

   After they are moved, nodes remain pinned. The icon appears in these objects.

Automatically arranging nodes on the topology map

For optimal arrangement of objects on the topology map, you can use an algorithm to automatically change the location of nodes (auto-arrange). This algorithm lets you arrange unpinned nodes that have links with other nodes according to the topological hierarchy.

To arrange nodes on the topology map:

Click the button in the toolbar located in the left part of the topology map display area.

After automatic arrangement, unpinned nodes will not be pinned in their new locations. If necessary, you can manually pin these objects.

Filtering objects on the topology map

To limit the number of nodes displayed on the topology map, you can use the features described below:

Filtering by device status

To filter objects on the topology map by device status:

1. In the toolbar above the topology map, open the **Device statuses** drop-down list.

   You will see a list containing the names of statuses for known devices (*Unauthorized*, *Authorized*, and *Archived*) and the *Unmanaged switch* status for unmanaged switches.

2. In the drop-down list, select the check boxes for the statuses of devices that need to be displayed on the topology map.

3. Click **OK**.

The topology map will display only those nodes that have the selected statuses.

Filtering by device security state

To filter objects on the topology map by device security state:

1. In the toolbar above the topology map, open the **Device states** drop-down list.

   You will see a list containing the names of security states for devices (*OK*, *Warning*, and *Critical*).

2. In the drop-down list, select the check boxes for the security states of devices that need to be displayed on the topology map.

3. Click **OK**.

The topology map will display only those nodes that represent devices with the selected security states.

Filtering by device category

To filter objects on the topology map by device category:

1. In the toolbar above the topology map, open the **Device categories** drop-down list.

   You will see a list containing the names of categories for known devices, as well as an individual category for unmanaged switches.

2. In the drop-down list, select the check boxes for the categories of devices that need to be displayed on the topology map.

3. Click **OK**.

The topology map will display only those nodes that represent the selected categories of devices.

Filtering by VLAN ID in topology settings

To filter objects on the topology map by VLAN ID in topology settings:

1. In the toolbar above the topology map, open the **VLAN ID** drop-down list.

   You will see a window containing a field for entering VLAN IDs.

2. Enter one or more VLAN IDs of devices that need to be displayed on the topology map.

   You can specify several identifiers separated by comma or as a range (for example: `1, 2, 4-6, 8`).

3. Click **OK**.

   The topology map will display only those nodes whose topology settings include ports with the defined VLAN IDs.

Enabling and disabling the display of nodes that do not have links to other nodes

By default, the topology map displays all nodes regardless of whether they have links to other nodes. If necessary, you can disable the display of all nodes that do not have links with other nodes on the topology map.

To enable or disable the display of nodes that do not have links to other nodes:

Use the **Display unlinked nodes** toggle switch in the toolbar located above the topology map.

Resetting the filter settings

You can reset the defined node filtering settings to their default state.

To reset the defined filter settings on the topology map:

In the toolbar located above the topology map, click **Default filter** (this button is displayed if filter settings have been defined).

Saving and loading topology map display settings

This section describes the topology map display customization features.

The application lets you save the current topology map display settings. A set of saved display settings is called a *view*. You can use views to apply their saved settings on the topology map (for example, to quickly restore the display settings after making some changes, or to work with the topology map on a different computer).

When a topology map view is saved, the following display settings are saved:

- Scale
- Positioning of the topology map
- Location of pinned nodes
- Filtering of nodes

The application can save and use no more than 10 groups of settings providing different topology map views.

All users can manage the list of topology map views (including saving the current display settings).

Adding a new view while saving the current topology map display settings

To add a new view while saving the current topology map display settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Topology map** tab in the **Network map** section, configure the topology map display settings.
3. Open the **Configure network map views** window by clicking **Manage views**.
4. Click **Add**.
5. Type the view name in the entry field.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A view name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 100 characters or less.
   - Must not match the name of a different view (not case-sensitive).
6. Click the ✓ icon on the right of the entry field.

Updating a view while saving the current topology map display settings

To update a view while saving the current topology map display settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Topology map** tab in the **Network map** section, configure the topology map display settings.
3. Open the **Configure network map views** window by clicking **Manage views**.
4. Select the view in which you want to save the current topology map display settings.
5. Click **Overwrite**.

   A window with a confirmation prompt opens.
6. In the prompt window, confirm that you want to save the current settings in the selected view.

Renaming a topology map view

To rename a topology map view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network map** tab in the **Topology map** section, open the **Configure network map views** window by clicking **Manage views**.
3. Select the view that you want to rename.
4. Click the icon on the right of the current view name.
5. In the entry field, enter the new name of the view.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   A view name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 100 characters or less.
   - Must not match the name of a different view (not case-sensitive).
6. Click the icon on the right of the entry field.

Deleting a topology map view

To delete a topology map view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network map** tab in the **Topology map** section, open the **Configure network map views** window by clicking **Manage views**.
3. Select the view that you want to delete.
4. Click **Delete**.

   A window with a confirmation prompt opens.
5. In the prompt window, confirm deletion of the selected view.

Applying saved view settings on the topology map

To apply saved view settings on the topology map:

1. On the **Network map** tab in the **Topology map** section, open the **Configure network map views** window by clicking **Manage views**.
2. Select the relevant view in the list.
3. Click **Apply**.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm application of the view.

Search for nodes on the topology map

You can search nodes on the topology map based on information about these nodes. This search will involve all nodes that meet the current filter settings, including those located outside of the displayed part of the topology map.

For nodes representing known devices, the search is performed in all columns of the table of devices except **Status**, **Security state**, **Last seen**, **Last modified**, and **Created**. The search is also performed in the values of custom fields for devices.

To find relevant nodes on the topology map:

On the **Topology map** tab in the **Network map** section, enter your search query into the **Search nodes** field. The search is initiated as you type characters in the search field.

If nodes that satisfy the search query are found, the contours of these nodes are highlighted in yellow. Meanwhile, the right part of the **Search nodes** field will display the following items:

- Sequence number of the currently selected node among the search results.
- Total number of nodes found.
- Arrows for moving between found nodes. Arrow movements proceed in alphabetical order of the names of found objects. When moving to the next node, the topology map is automatically positioned to display this node.

Configuring event types

Event types define the settings used when registering events, including their titles, descriptions, base scores, and registration settings. In Kaspersky Industrial CyberSecurity for Networks, you can view the settings of event types, change the settings of event types, and configure automatic saving of traffic and transmission of registered events via connectors.

Viewing the table of event types

The event types provided in the application are displayed under **Settings** → **Event types** in the application web interface.

The table of event types contains *system event types*. These event types are created by the application during installation and cannot be deleted from the list. Various sets of system event types are used for the event registration technologies employed in the application.

Some system event types can be used as the basis for configuring *user-defined settings of events* that will be used when registering events in specific cases. User-defined settings can be defined for the following event types:

- Event type based on Deep Packet Inspection technology with the code 4000002900 – for registering events based on Process Control rules.
- Event type based on External technology with the code 4000005400 – for registering events using the Kaspersky Industrial CyberSecurity for Networks API.

User-defined settings take priority when registering events. The settings defined in system event types are used if there are no user-defined settings.

The following settings are available for event types:

- **Code** – unique number (identifier) of the event type. In the event types table, the number is displayed together with the event title in the **Title template** column. In the table of registered events, the event type identifier is displayed in the **Event type** column.
- **Title** – contents of the event title presented as text and/or variables. System event types may utilize specific variables only for these event types (for example, the `$systemCommandShort` variable in the event type for Command Control technology) or common variables that can also be used in user-defined settings (for example, the `$top_level_protocol` variable in the event type for Network Integrity Control technology). In the event types table, the content of the title is displayed together with the event type number in the **Title template** column. In the table of registered events, the text of the title and/or received values of variables are displayed in the **Title** column.
- **Base score** – initial value for calculating the score of the registered event. If an event type can have different base scores, then the maximum value is displayed. This setting is displayed in the event types table.
- **Technology** – technology used for event registration. This setting is displayed in the event types table.
- **Description** – additional text that describes the event type. Like the title, a description may contain variables. This setting is not displayed in the event types table (you can view the description in the details area of the selected event type). In the table of registered events, the text of the description and/or received values of variables are displayed in the **Description** column.
- **<Recipient connector name>** – name of the connector that the application uses to forward events to the recipient system. The application sends recipient systems only those event types that are configured for forwarding through the connector. Each connector configured to forward events to the third-party systems is displayed in a separate column of the risk types table. This setting is not displayed in the details area for the selected event type.

- **Event regeneration period** – maximum period of time after which an event enrollment is allowed again. If the conditions for event enrollment are repeated before the specified time period elapses, a new event is not registered but the counter for the number of repeats of the previously registered event is increased and the date and time of the last occurrence of the event is updated. After this period elapses, the application will register a new event of this type when the event registration conditions are repeated. The repeat event timeout period begins when an event of this type is last registered. For example, if the defined time period is 8 hours and the conditions for registering this type of event are detected two hours after the previous event, a new event will not be registered. A new event will be registered when the event registration conditions are detected after 8 or more hours. This setting is not displayed in the event types table (you can view and configure this setting in the details area of the selected event type).

  For registered events, the event regenerate period may occur earlier than the specified period. Re-registration of an event is allowed earlier than the defined period if a status of *Resolved* is assigned to the event, and if the computer performing Server functions was restarted.

- **Save traffic** – this setting enables or disables automatic saving of traffic when an event is registered. This setting is not displayed in the event types table (you can view and configure this setting in the details area of the selected event type).

  If automatic saving of traffic is disabled, you can manually load traffic some time after registration of an event of this type. When the application receives a request to load traffic, it searches network packets in traffic dump files that were temporarily created by the application. If relevant network packets are found in the traffic dump files, they are loaded after first being saved in the database.

When viewing the event types table, you can use the configuration, filter, search, and sorting functions.

Editing the settings of a system event type

To edit the settings of a system event type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Event types**.
3. In the table of event types, select the event type that you want to edit.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. Configure the editable settings, such as the event regeneration period and settings for saving traffic.
6. Click **Save**.

Configuring automatic saving of traffic for system event types

When editing event types, you can enable or disable automatic saving of traffic for events when they are registered. If traffic saving is enabled, the network packet that caused the event registration is saved to the database, as well as the packets received before and after the event registration and detected within the network session in which the event was registered. The settings for saving traffic determine the number of saved network packets and time limits.

If automatic saving of traffic is disabled for an event type (and user-defined settings enabling autosaving of traffic are not defined for this event type), you will be able to manually load traffic only after waiting some time after registration of an event of this type. In this case, the application uses traffic dump files to load traffic (these files are temporarily saved and are automatically deleted as more and more traffic is received). When traffic is loaded from these files, the database saves the specific amount of network packets that was defined by default when enabling the saving of traffic for event types.

The application saves traffic in the database only when an event is registered. If the conditions for registering this event are repeated during the event regenerate timeout, traffic at this point in time is not saved in the database.

You can enable and configure the saving of traffic for any event types except a system event type assigned the code 4000002700. An event with the code 4000002700 is registered when there is no traffic at a monitoring point. For this reason, traffic is not expected for this type of event.

If saving of traffic is enabled for incidents (meaning for a system type of event that is assigned the code 8000000001), the application saves traffic for all embedded events of an incident when the incident is registered. The settings defined for the incident are applied when saving traffic of embedded events. However, the traffic storage settings defined directly for event types embedded in an incident take priority over the settings defined for an incident. This means that traffic for embedded events of an incident will be saved according to the settings defined for the specific types of these events. If these settings are not defined, the traffic for embedded events will be saved according to the settings defined for an incident.

To enable and configure the settings for saving traffic for an event type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Event types**.
3. In the table of event types, select the event type that you want to edit.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. Set the **Save traffic** toggle switch to *Enabled*.
6. Configure saving of traffic before event registration. To do so, specify relevant values in **Total packets before event** and/or **Time to event, ms**. If the value is zero, the setting is not applied. If the values are defined in both of these fields, the application will save the minimum amount of packets corresponding to one of the defined values.

7. Configure the saving of traffic after event registration. To do so, specify the relevant values in **Total packets after event** and/or **Time after event, ms**. If the value is zero, the setting is not applied. If the values are defined in both of these fields, the application will save the minimum amount of packets corresponding to one of the defined values.

   For certain technologies (particularly Deep Packet Inspection), fewer post-registration packets than defined by the settings for saving traffic may be saved in events. This is due to the technological specifics of traffic monitoring.

8. Click **Save**.

Configuring forwarding of events via connectors

When configuring system event types, you can specify the connectors through which Kaspersky Industrial CyberSecurity for Networks will forward registered events to recipient systems (for example, to Kaspersky Security Center). Kaspersky Industrial CyberSecurity for Networks can relay event information through multiple connectors simultaneously.

To configure forwarding of events through connectors to recipient systems:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Event types**.
3. Make sure that the event types table displays columns with the relevant connectors.

   If a column with the required connector is not available, check the column display settings. If the connector has not been added to the list of connectors, add it.

4. In the event types table, select the event types for which you want to enable or disable forwarding via connectors.

   If you select one event type, the details area appears on the right part of the web interface window.

5. Do one of the following:

   - If you select one event type, click **Select connectors** in the details area.
   - If you select several event types, click **Select connectors** in the upper part of the window.

   The **Event recipient connectors** window opens.

6. Select the check boxes next to those connectors that you want to use to forward events to recipient systems. If you want to disable forwarding of events through a connector, clear the check box next to this connector.
7. Click **OK**.

   In the event types table, check boxes appear in the cells of the columns for the connectors that were selected for forwarding events.

Common variables for substituting values in Kaspersky Industrial CyberSecurity for Networks

You can use common variables to substitute current values in Kaspersky Industrial CyberSecurity for Networks. You can use common variables in the following settings:

- Titles and descriptions of events in user-defined settings for registering events (for example, in Process Control rules).
- Settings for forwarding events, application messages or audit entries via the email connector.

To insert a common variable into the entry field:

Start entering the name of the variable beginning with the $ character and choose the appropriate common variable in the list that appears.

Depending on their purpose, common variables can be used to substitute values in various settings (see the table below).

Common variables for value substitution

Variable	Purpose	Where it is used
`$closed`	Date and time when a status of *Resolved* was assigned or the date and time of the event regeneration period (for events that are not incidents), or the date and time of registration of the last event included in the incident (for incidents).	• Settings for forwarding events through a connector.
`$communications`	Strings describing network interactions (one line for each network interaction) indicating the protocol and addresses of the network packet source and destination.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$count`	Number of times an event or incident was triggered.	• Settings for forwarding events through a connector.
`$description`	Description	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$dst_address`	Address of the network packet destination (depending on the data available in the protocol, this can be an IP address, port number, MAC address and/or other address data).	• User-defined settings for registering events.
`$extra.<paramName>`	Additional variable added using the `AddEventParam` function for an external system or Lua script, or resulting from `SELECT` in the SQL query of a Network Anomaly Detection rule	• User-defined settings for registering events.
`$id`	Unique ID of the registered event, application message, or audit entry.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$message_category`	Category of transmitted data (event, application message, or audit entry).	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$message_count`	Number of transmitted events, application messages or audit entries.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$messages`	Template that consists of a block containing a list of data.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$monitoring_point`	Name of the monitoring point whose traffic invoked registration of the event.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$msg_line_templ`	Email notification string template	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$node`	Node with the installed application component that sent the data.	• Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$occurred`	Date and time of registration.	• User-defined settings for registering events. • Settings for forwarding events

		through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$protocol`	Name of the application-layer protocol that was being monitored when the event was registered.	• User-defined settings for registering events.
`$result`	Operation result in the audit entry.	• Settings for forwarding audit entries through a connector.
`$rule_description`	Network Anomaly Detection rule description	• User-defined settings for registering events.
`$rule_max_value`	Assigned maximum value in the Process Control rule.	• User-defined settings for registering events.
`$rule_min_value`	Assigned minimum value in the Process Control rule.	• User-defined settings for registering events.
`$rule_name`	Network Anomaly Detection rule name	• User-defined settings for registering events.
`$rule_values`	List of values of the Process Control rule (authorized or unauthorized).	• User-defined settings for registering events.
`$scanned_interval`	The time interval for which network sessions were analyzed	• User-defined settings for registering events.
`$score`	Event score value.	• Settings for forwarding events through a connector.
`$severity`	Event severity level.	• Settings for forwarding events through a connector.
`$src_address`	Address of the network packet source (depending on the data available in the protocol, this can be an IP address, port number, MAC address and/or other address data).	• User-defined settings for registering events.
`$status`	Application message status.	• Settings for forwarding application messages through a connector.
`$system_process`	Application process that invoked message registration.	• Settings for forwarding application messages through a connector.
`$tags`	List of all names and values of tags indicated in the Process Control rule.	• User-defined settings for registering events.
`$technology`	Technology associated with the event.	• Settings for forwarding events through a connector.
`$technology_rule`	Name of the rule in the event.	• User-defined settings for registering events. • Settings for forwarding events through a connector.
`$template_name`	Name of the template in the Network Anomaly Detection rule	• User-defined settings for registering events.
`$title`	Event title, message text, or registered action.	• Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$top_level_protocol`	Name of the top-level protocol.	• User-defined settings for registering events.
`$type_id`	Code of the event type, application message, or audit entry.	• User-defined settings for registering events (the `$event_type_id` variable may also be used). • Settings for forwarding events through a connector. • Settings for forwarding application messages through a connector. • Settings for forwarding audit entries through a connector.
`$user`	Name of the user that performed the registered action.	• Settings for forwarding audit entries

		through a connector.

Configuring risk types

Risk types define the settings used when registering risks in Kaspersky Industrial CyberSecurity for Networks: names, categories, and base scores for risks. You can view the settings of risk types and edit the values of base scores for certain types of risks if necessary.

After the application is installed, the original list of risk types is used. You can update and expand the supported risk types by installing updates.

Viewing the table of risk types

The table of risk types is displayed under **Settings** → **Risk types** in the application web interface.

The settings of risk types are displayed in the following columns of the table:

- **Code**

  Unique number of the risk type. In the table of registered risks, the number of a risk type is displayed in the details area of the selected risk.

- **Name**

  The name of the risk type displayed in the risk type table. When a risk is registered, its name may not fully match the name of the risk type used. The names of some risk types can be completely replaced by other names for registered risks. For instance, risk types with such names include risks of the **Risk from external system** types. If this type of risk is used to register a risk, the application saves the risk name specified in the risk information source (for example, in a third-party application that uses Kaspersky Industrial CyberSecurity for Networks API).

- **Category**

  Name of the risk category.

- **Base score**

  Initial value for calculating the score of the registered risk. The defined values for base scores are applied when registering all risks except risks from external systems. Risk types named **Risk from external system** have zero values for their base scores. The base scores for these risks must be specified in the recipient applications that register risks using the Kaspersky Industrial CyberSecurity for Networks API.

When viewing the table of risk types, you can use the configuration, filter, search, and sorting functions.

Changing the base score for a risk type

Base scores cannot be changed for risk types named **Risk from external system**. If such a risk type is used to register a risk, the base score of this risk must be defined from the source of information about the risk (for example, by the recipient application using the Kaspersky Industrial CyberSecurity for Networks API).

To change the base score for a risk type:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Select **Settings** → **Risk types**.
3. In the table of risk types, select the risk type whose base score you want to edit.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. Specify the necessary value for the base score.
6. Click **Save**.

Managing the settings for storing risks

You can change the limits on the maximum space used for storing risks.

To edit risk storage settings:

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

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

   The details area will show the tabs for configuring the Server parameters.
5. On the **General** tab, go to **Risks** and use the **Max volume** setting to define the size limit for storing risks data.

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

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.
6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for risks, and specify the minimum number of days.
7. Click **Save**.

Managing sets of rules for vulnerability and compliance audit jobs

You can manage sets of vulnerability and compliance audit job rules on the **Rule sets** tab in the **Security audit** section. After database and application module updates are installed, the system sets of rules for vulnerability and compliance audit jobs are used by default.

Users with the Administrator or Security Officer role can manage sets of rules for vulnerability and compliance audit jobs.

Vulnerability and compliance audit rules

Kaspersky Industrial CyberSecurity for Networks supports vulnerability and compliance audit rules written in the following languages:

- OVAL (Open Vulnerability and Assessment Language) is an open language for describing vulnerabilities and assessing configurations of information systems. The language standardizes the ways of presenting information, the process of analyzing the system, and the format of the result.

  Rules that use only this language are OVAL definitions which formalize the requirements for information systems, providing the capability to automatically process these requirements.

- XCCDF (Extensible Configuration Checklist Description Format) is an XML-based language for describing checklists of security settings. XCCDF documents usually contain sets of information system requirements.

  Rules that use this language are the lists of high-level requirements in the form of documents with profiles and data groups. For automated processing, such rules must contain associated OVAL definitions.

Vulnerability and compliance audit rules are grouped into sets. You can use the following types of rule sets:

- System rule sets. These rule sets are supplied and updated together with the database and application module updates. To use system rule sets, install the updates.

  > System rule sets contain descriptions developed by both Kaspersky and third-party organizations. Descriptions and wordings obtained from third-party organizations and included in system rule sets may be distributed as is.

- User-defined rule sets. These rule sets are loaded into the application by the user through the import of files.

When a rule set is loaded, the application verifies the rules in the rule set. If errors are detected in the verified rules, the application blocks these rules from being applied. If errors are detected in all rules of the set or the set does not contain any rules, the application blocks the entire set from being applied.

When creating or editing vulnerability and compliance audit jobs, you can select the rules according to which scans are performed.

Viewing the table of vulnerability and compliance audit rule sets

The vulnerability and compliance audit rule set table is displayed on the **Rule sets** tab in the **Security audit** section.

The rule set settings are displayed in the following columns of the table:

- **ID**

  Rule set ID assigned by Kaspersky Industrial CyberSecurity for Networks.

- **Name**

  The name by which the rule set is represented in the application.

- **Description**

  Description of the rule set.

- **Publisher**

  Name of the XCCDF document publisher (if specified).

- **XCCDF document version**

  Information about the XCCDF document version (if specified).

- **XCCDF status**

  The final status specified for the XCCDF document.

- **XCCDF profiles**

  The number of profiles in the XCCDF document.

- **XCCDF rules in set**

  The number of rules in the XCCDF document.

- **OVAL definitions**

  The number of OVAL definitions.

- **Created**

  Date and time when the rule set was added to the application.

- **Changed**

  Date and time when the rule set was last modified in the application.

- **Source**

  The type of rule set that determines how the rule set is loaded into the application: system or user rule set.

When viewing the rule set table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Importing vulnerability and compliance audit rule sets

You can import vulnerability and compliance audit rules from files to Kaspersky Industrial CyberSecurity for Networks. Files can contain rules written in the OVAL language or in the XCCDF language using OVAL definitions.

Imported rule sets are called *custom* rule sets. For these rule sets, **Source** is set to **User**.

To import files, they must be packed into a ZIP archive. Supported options for the contents of the ZIP archive:

- XCCDF package files that represent an XCCDF document and OVAL definitions in XML format. If the package includes dictionary files in the CPE (Common Platform Enumeration) format, these files must also be added to the archive.

  The files must be located at the root of the archive. The names of the files in the archive must match the following name masks:

  - `*-xccdf.xml` – mask for the name of the XCCDF document file (for example, SCAP1-xccdf.xml)
  - `*-oval.xml` – mask for the name of the file with OVAL definitions (for example, SCAP1-oval.xml)
  - `*-cpe-dictionary.xml` – mask for the name of the CPE dictionary file (for example, SCAP1-cpe-dictionary.xml)
  - `*-cpe-oval.xml` – mask for the name of the file with OVAL definitions and CPE dictionary (for example, SCAP1-cpe-oval.xml)

- A file that contains OVAL definitions and is not part of an XCCDF package (the XCCDF document is not required to use the file).

  The file must be located at the root of the archive. The name of the file in the archive must match the mask: `*-oval.xml` (for example, SCAP2-oval.xml).

To import a set of vulnerability and compliance audit rules:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Security audit** section.
3. On the **Rule sets** tab, click **Import** in the toolbar.
4. Click **Browse** and specify the local path to the ZIP archive.
5. Click **Import**.

   The data import process starts. Information about the running import operation is displayed in the list of background operations.
6. To switch to a new rule set, perform the following actions:

   a. Click in the application web interface menu.

   The list of background operations opens.

b. Wait for the import operation to complete.

c. Click **Show**.

Changing vulnerability and compliance audit rule sets

You can modify names and text descriptions of the custom vulnerability and compliance audit rule sets. Such changes are not available for system rule sets.

To change the name or the text description of a rule set:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Security audit** section.
3. On the **Rule sets** tab, select the relevant rule set.

   The details area appears in the right part of the web interface window.
4. Click **Edit**.
5. Enter a name and a description for the rule set.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . ' - " _`. The rule set name must begin and end with any permitted character except space.

   The rule set name must contain no more than 1024 characters. The rule set description must contain no more than 4096 characters.
6. Click **Save**.

Deleting vulnerability and compliance audit rule sets

You can delete custom and system vulnerability and compliance audit rule sets. However, you cannot delete rule sets that have associated jobs.

To delete rule sets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using an Administrator or Security Officer account.
2. Select the **Security audit** section.
3. On the **Rule sets** tab, select the rule sets that you want to delete.
4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm the deletion of the rule sets.

   You can delete only the rule sets that have no associated vulnerability and compliance audit jobs. If there are rule sets with associated jobs among the selected rule sets, a corresponding message appears. To delete such rule sets, first delete the associated jobs.

Managing account credentials secrets for remote connections

Secret storage is implemented in Kaspersky Industrial CyberSecurity for Networks. *Secrets* allow you to securely store and use identification and authentication information that the application needs for automatic remote connections to devices. Secrets are used in security audit jobs that have the **Remote connection** device polling method selected or an **Active Poll** connector configured.

The application provides for various types of secrets. Depending on the purpose of the secret, you can select a relevant type and enter the appropriate data when adding or editing the secret settings.

Keep in secret the credentials required for remote connections to devices using remote connection protocols. The security audit jobs that use the **Remote connection** method to poll devices use the SSH protocol for remote connections. The **Active poll** connectors can use various protocols for remote connections, depending on the selected polling methods.

To ensure that identification and authentication details stored in secrets are used securely, the application implements protection against compromise of secrets when connected to remote devices. After public keys received from devices are saved in the application, it monitors all subsequent remote connections to these devices and sends no information from secrets in the event of device spoofing on the network.

Critical secret information, such as a password or private key for authentication, is available to you as plain text only one time: while you enter this information when creating the secret. Once a secret is saved, critical information cannot be viewed. You can only replace critical information in the secret when you change the secret, for example, enter a new password.

You can manage secrets in the **Settings** → **Secrets** section. No more than 500 secrets can be added to the application.

Users with any role except the Operator role can manage secrets.

Adding a secret

You can add secrets to the application secrets storage.

To add a secret:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select **Settings** → **Secrets**.

3. Open the details by clicking **Add secret**.

4. Enter the secret name.

   The secret name must be unique (must not match the names of other secrets) and must contain up to 256 characters. You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } / \ : ; , . - _`. The secret name must begin and end with any permitted character except space.

5. Select the type of secret and configure its settings.

   You can select the following types of secrets:

   - **Password only**: this type of secret is used if only the password of a user with the relevant permissions is required for the access to device configuration data.

   - **User name and password**: this type of secret is used if a user name and password are required to receive data from the device.

   - **User name and password, root password**: this type of secret is used if a user name and password are required to receive data from the device, and the root password or the password for an account that processes requests with administrator privileges is additionally required for a connection with administrator (root) privileges.

   - **User name and password, encryption password**: this type of secret is used if a user name and password are required to receive data from the device, and an encryption password is additionally required to establish encrypted connections.

   - **Mixed**: this type of secret is used for the **Remote connection** device polling method in vulnerability and compliance audit jobs or in configuration control jobs. You can specify the following settings for this type of secret:

     - User name to be used for remote connections to devices.

       A user name can contain Latin characters, numbers, periods, and the following special characters: `_` and `-`. The name must begin with a letter, and end with any supported character except a period.

     - **User password**: if the user password will be used for authentication.

       The password must contain up to 256 ASCII characters.

     - **Private key**: if the private key will be used for authentication.

       You can manually enter the sequence of characters comprising the key or upload the key from a file by clicking **Copy from file**. Files in the CRT, PEM, CER formats are supported for uploading private keys. If the private key file is protected by a password phrase, enter the password phrase in the **Passphrase** field before uploading the key.

       > To use the private key, copy the corresponding public key to all devices to which the remote connections using the secret will be established. Copying the public key to devices is performed without the participation of Kaspersky Industrial CyberSecurity for Networks.

       Root user password: if an additional password is required for connections to network equipment with administrator (root) privileges. In such cases, access is requested on behalf of the root account or on behalf of the account that is set on the network equipment to process requests with administrator privileges.

6. Click **Created**.

Viewing the secret table

The table of remote connection secrets is displayed in the **Settings** → **Secrets** section of the application web interface.

Information about secrets is displayed in the following columns of the table:

- **Name of secret**

  Name used to represent the secret in the application.

- **Created**

  Date and time when the secret was added to the application.

- **Changed**

  Date and time when the secret was last modified in the application.

When viewing the secrets table, you can use the configuration, filter, search, and sort functions.

Protecting against compromise of secrets when connected to remote devices

Identification and authentication details from secrets should be used only for remote connections to those devices selected for security audit jobs. To protect this information against possible compromise in the event of device spoofing, the application checks the public key received from the device before sending the information. The device uses the public key to establish SSH connections. A public key helps the application to verify that the SSH connection is being established with the correct device. Identification and authentication details are sent to the device after verifying that the received public key matches the public key saved in the application.

The saved public key of the device is displayed in the details area of the selected device on the **General** tab.

Receiving and saving devices' public keys in the application

Public keys of devices are not defined in Kaspersky Industrial CyberSecurity for Networks by default. A device's public key is received and saved when an SSH connection is first established with the device for scanning as part of a security audit job that uses **Remote connection** polling or an **Active Poll** connector. Identification and authentication details from the selected secret are sent to the device without checking the received public key. Therefore, before starting the security audit job for the first time for the selected device and establishing an SSH connection to it, make sure that there is no spoofed device on the network. To do this, you can run `ifconfig` to check that the device IP addresses defined in the application match those on the actual device network interfaces.

Resetting saved device public keys

SSH connection keys on devices may change with time. Device users may generate new keys when their current private keys are at a risk of compromise.

When the private key is changed on the device, the public key is changed as well. After changing the public key, the application stops sending information from the secrets to this device because the new public key no longer matches the one saved in the application. Therefore, any subsequent device scans as part of security audit jobs finish with an error.

After changing the public key on the device, reset the currently saved public key for the device stored in the application. This will allow the secrets to be used again when connecting to the device remotely.

After resetting the saved public key, the application saves the newly received public key when an SSH connection is next established with this device. Check that there is no spoofed device on the network, similarly to when initially receiving and saving a public key.

Users with any role except the Operator role can reset saved device public keys.

To reset saved device public keys:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Assets** section.

3. On the **Devices** tab, select the devices you want to reset the saved public keys for.

4. Right-click to open the context menu of one of the selected devices.

5. In the context menu, select **Reset public key**.

   A window with a confirmation prompt opens.

6. In the prompt window, click **OK**.

Changing the settings of a secret

When editing the secret settings, you can change its type and/or set different credentials.

After the secret settings, including the secret name, are changed, the new settings are applied in the security audit jobs where the secret is used. If you change the secret type, errors may occur during subsequent job runs if the new secret type does not match the job settings.

To edit the secret settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select **Settings** → **Secrets**.

3. Select the secret you want to change.

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

4. Click **Edit**.

5. Change the settings as necessary. The options available when changing the secret settings are the same as the ones when adding a secret.

   Critical secret information, such as passwords and a private key for authentication, is not displayed as plain text. You can only replace the critical information with new information by using the links above the credentials fields.

Deleting secrets

You can delete secrets from the Kaspersky Industrial CyberSecurity for Networks secrets repository.

Before deleting a secret, it is recommended to specify a different secret or polling method in the security audit jobs that use this secret. If a deleted secret is specified in the security audit job, errors occur the next time the job is run.

To delete secrets:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select **Settings** → **Secrets**.

3. Select the secrets you want to delete.

4. Click **Delete**.

   A window with a confirmation prompt opens.

5. In the prompt window, confirm the deletion of the secrets.

Managing reports and report templates

Kaspersky Industrial CyberSecurity for Networks can generate reports containing information about the states of devices and system security, monitored technological process parameters and system commands, and information about detected risks and interactions with third-party devices. The application generates such reports based on *report templates*. A report template is a set of parameters determining the conditions for generating a report. Templates can be system templates (created during installation of the application) or user-defined templates (created by duplicating templates).

In the **Reports** section, a user with the Administrator of Security Officer role can duplicate templates to create user-defined report templates, edit and delete report templates, delete generated reports, and cancel report generation.

Reports are saved in PDF format.

Kaspersky Industrial CyberSecurity for Networks can also generate reports with the device scan results as part of a vulnerability and compliance audit job, as well as reports on the runs of the entire vulnerability and compliance audit job. Reports generation is started in the **Security audit**. You can view generated reports on the **Generated reports** tab.

Duplicating a report template

In the current version of Kaspersky Industrial CyberSecurity for Networks, you can create user-defined templates by duplicating existing report templates. You can duplicate system templates and user-defined templates. When duplicating a template, you cannot change the composition and layout of information blocks in a report.

The maximum number of templates in the application is 5000.

Users with the Administrator or Security Officer role can duplicate report templates.

To duplicate a report template:

1. Select the **Reports** section.
2. On the **Report templates** tab, select the relevant template.

   The details area appears in the right part of the web interface window.
3. Click **Create new template**.
4. In the **Name** field, enter the name of the report template.

   You can use letters of the English and Russian alphabets, numerals, a space, and the characters -, – and _.

   The report template name must meet the following requirements:

   - Must not match the name of another report template (not case-sensitive).
   - Must contain 100 characters or less.

   The names of reports generated based on the updated template will match the new name of the template.
5. In the **Data period** drop-down list, select the time period for which you want to obtain system information in the report.

   You can generate reports containing information received by the application over the past 24 hours, 7 days, 30 days, year, or a manually defined period.
6. If you need to generate reports according to a schedule, turn on the **Generating a report by schedule** toggle switch and set up a schedule:

   a. In the **Frequency** drop-down list, choose how often to generate a report: **Hourly**, **Daily**, **Weekly**, or **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise time to start report generation.

7. If necessary, use the **Destination addresses** field to enter the email address to which you want to send the generated reports. If you need to specify additional recipients of the report, click **Add destination address** and enter the email address.

   The maximum number of report recipients is 20.

8. Click **Save**.

The new report template will appear in the report templates table.

Editing a report template

Users with the Administrator or Security Officer role can edit report template settings.

To edit report template settings:

1. Select the **Reports** section.
2. On the **Report templates** tab, select the relevant template.

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

3. Click **Edit**.
4. In the **Name** field, enter the name of the report template.

   You can use letters of the English and Russian alphabets, numerals, a space, and the characters -, – and _.

   The report template name must meet the following requirements:

   - Must not match the name of another report template (not case-sensitive).
   - Must contain 100 characters or less.

   The names of reports generated based on the updated template will match the new name of the template.

5. In the **Data period** drop-down list, select the time period for which you want to obtain system information in the report.

   You can generate reports containing information received by the application over the past 24 hours, 7 days, 30 days, year, or a manually defined period.

6. If you need to generate reports according to a schedule, turn on the **Generating a report by schedule** toggle switch and set up a schedule:

   a. In the **Frequency** drop-down list, choose how often to generate a report: **Hourly**, **Daily**, **Weekly**, or **Monthly**.

   b. Depending on the selected option, specify the values for the settings to define the precise time to start report generation.

7. If necessary, use the **Destination addresses** field to enter the email address to which you want to send the generated reports. If you need to specify additional recipients of the report, click **Add destination address** and enter the email address.

   The maximum number of report recipients is 20.

8. Click **Save**.

The changes will be displayed in the corresponding columns of the report templates table.

Deleting a report template

Only user-defined report templates can be deleted.

Users with the Administrator or Security Officer role can delete report templates.

To delete a report template:

1. Select the **Reports** section.
2. On the **Report templates** tab, select one or more report templates that you want to delete.
3. Click **Delete**.

   You cannot delete system report templates. In the report templates table, system templates are displayed with the icon.

4. In the opened prompt window, confirm deletion of the report templates.

Deleting a report

Users with the Administrator or Security Officer role can delete reports in the application.

To delete a report:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select one or more reports that you want to delete.

   Reports in the reports table are filtered based on the IDs of reports that were last run in the current Server connection session. To display all generated reports, reset the filter settings by clicking **Default filter**. If necessary, you can configure filtering based on a specific period of time.

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

3. Click **Delete**.
4. In the opened prompt window, confirm deletion of the report.

Canceling report generation

You can cancel report generation only for a report with a status of **In progress**.

If necessary, a user with the Administrator or Security Officer role can cancel generation of reports started by any user of the application.

To cancel generation of a report:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select the report with a status of **In progress** that you want to cancel.

   The details area appears in the right part of the web interface window.
3. Click **Cancel**.
4. In the opened prompt window, confirm cancellation of report generation.

After this request is fulfilled, the report status changes to **Canceled**.

Managing the settings for storing report files

You can change the limits on the maximum space used for storing report files.

To edit the report file storage settings:

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

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

   The details area will show the tabs for configuring the Server parameters.
5. On the **General** tab go to the **Reports** settings group and use the **Max volume** setting to define a limit for the space used to store report files.

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

   When changing the value of this setting, you need to keep in mind that the sum of all volume limits cannot exceed the defined maximum storage volume for the node.
6. If necessary, use the **Storage time (days)** setting to enable a minimum storage time for report files, and specify the minimum number of days.
7. Click **Save**.

Managing a security policy

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

- User-defined sets of Intrusion Detection rules
- Network Anomaly Detection rules and dictionaries
- Allow rules for Interaction Control and for events
- Settings of devices and tags that are used for Asset Management and Process Control
- Network map display settings
- User settings on devices
- Application and patch settings on devices
- Address space settings
- Event types settings
- Risk types settings

All other application settings are not part of a security policy and are applied separately from it. This includes the settings of nodes that have components installed, the list of application users, objects linking events and devices in the table of devices, and other settings.

A security policy is stored on the Server and is automatically updated each time application settings are modified (for example, when Interaction Control rules are added).

You can export a security policy to files and import them from files. You can also clear the current security policy on the Server to delete all previously saved settings.

When exporting, importing or clearing a security policy, you can select specific sections of the policy that you want to export, import, or clear. For example, you can export only devices and allow rules.

When exporting a security policy, the application creates a file containing information about the selected application settings. To import settings, you can select a previously exported file.

Changing the contents of a security policy file may result in a malfunction of Kaspersky Industrial CyberSecurity for Networks if you import a security policy from this modified file. The application may stop performing protection functions for the industrial network.

Exporting a security policy in the Server web interface

When connecting to the Server via the web interface, you can export the settings included in a security policy to a file. You can export the entire security policy or its individual sections.

When necessary, you can then import the relevant application settings from the file containing the saved security policy.

To export the current security policy:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select **Settings** → **Security policy**.
3. Click **Export**.

   You will see the security policy tree in which you can select the necessary sections to export.
4. Select the check boxes for the relevant sections of the security policy.
5. Click **Export**.
6. If file generation takes a long time (more than 15 seconds), the operation is moved to the background. If this is the case, follow these steps to download the file:

   a. Click in the application web interface menu.

      The list of background operations opens.

   b. Wait for the file generation operation to complete.

   c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Exporting a security policy using the export utility

To export the settings included in a security policy, you can use the kics4net-cli security policy export utility. The utility exports the entire security policy to a file in a specified directory. When necessary, you can then import the relevant application settings from the file containing the saved security policy.

The utility is automatically installed at /opt/kaspersky/kics4net-cli/bin/ on the Server computer. You can use built-in operating system tools to configure kics4net-cli to run automatically to create regular security policy backups.

The utility connects to the application Server via a connector added to the application.

To prepare the application for using the security policy export utility, do as follows:

1. In the application, add the connector to be used by the security policy export utility to connect to the application Server. Specify the **Generic** system type for the connector.

   The application generates a new communication data package after the connector is added. The communication data package is an archive.
2. On the computer with kics4net-cli installed, prepare a directory to apply the contents of the communication data package.

To prepare the directory:

a. Create a random directory and copy the communication data package to it.

b. Go to the folder containing the communication data package copy and enter the following command to unpack it:

```
unzip <communication data package name>
```

The unpacked files will appear in the directory.

c. Enter the following command to create a clientcert.crt certificate file:

```
sudo openssl pkcs12 -in certificates.pfx -nodes -clcerts -nokeys -out clientcert.crt
```

When prompted for a password, enter the password to access the connector certificate. This is the password you set when adding the connector or when creating the new communication data package for the connector.

d. Enter the following command to create a clientcert.key file:

```
sudo openssl pkcs12 -in certificates.pfx -nocerts -nodes -out clientcert.key
```

When prompted for a password, enter the password to access the connector certificate.

e. Enter the following command to copy webserver.pem to the kics4net-cli certificates directory /var/opt/kaspersky/kics4net-cli/certs/:

```
sudo cp webserver.pem /var/opt/kaspersky/kics4net-cli/certs
```

3. On the computer with kics4net-cli installed, prepare a directory to save the exported files.

To prepare the directory:

a. Make a random directory. To save files to a network share via your computer's local file system, you can use the directory to save files to the network share.

b. If the directory is not nested inside /var/opt/kaspersky/kics4net/shared/, assign the kics4net user as the owner. To do so, enter the following command:

```
sudo chown kics4net:kics4net <directory path>
```

When updating the connector certificate, you will also need to replace the files obtained from the previous communication data package. Otherwise, the kics4net-cli utility will not be able to connect to the application Server due to an invalid certificate in the old files. To replace the files, use the new communication data package to repeat step 2 of the procedure described above.

To export the current security policy:

1. On the computer with kics4net-cli installed, open the operating system console and go to /opt/kaspersky/kics4net-cli/bin/.

2. Enter the following command in the command line:

```
sudo ./kics4net-cli exec exportsecuritypolicy \
--client-cert=<path to the clientcert.crt file> \
--client-key=<path to the clientcert.key file> \
--export-path=<path to the directory for saving files> \
--timeout=<timeout>
```

   where:

   - `exec` is the argument for running a command supported by the utility (mandatory parameter)
   - `exportsecuritypolicy` is the command for exporting a security policy to a file (mandatory parameter)
   - `<path to the clientcert.crt file>` is the full path and name of the clientcert.crt certificate file in the directory for applying the contents of the communication data package (mandatory setting).
   - `<path to the clientcert.key file>` is the full path and name of the clientcert.key file in the directory for applying the contents of the communication data package (mandatory setting).
   - `<target directory>` is the full path to the directory where the exported files will be saved (mandatory setting).
   - `<timeout>` is the command execution result timeout in seconds (900 seconds by default), which can be increased via this parameter if the previous export attempt failed due to a large volume of data in the security policy.

   Example

```
sudo ./kics4net-cli exec exportsecuritypolicy --client-cert=/home/user1/certs/clientcert.crt --client-key=/home/user1/certs/clientcert.key --export-path=/var/opt/kaspersky/kics4net/shared/policy/
```

   After the utility finishes, verify that the files are in the target directory.

3. If the resulting file has to be copied to another location, grant permission to copy the file. Only the owner has the permission by default. To grant the permission, enter the following command:

```
sudo chmod o+r <path to the policy file>
```

Importing a security policy from a file

You can import application settings from a file containing a saved security policy. For import, you can use the file that was obtained when exporting a security policy using one of the following methods:

- Connecting to the Server via web interface
- Using the export utility

When importing security policy sections, the application first clears the current contents of these sections and then imports data into these sections.

If a file contains multiple sections of a security policy, you can select the relevant sections to import.

A security policy cannot be imported if updates are currently being installed or if another import process is running.

Only users with the Administrator role can import a security policy from a file.

To import a security policy from a file:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Disable the use of all technologies and methods on the nodes of the Server, sensors and monitoring points.
3. Select **Settings** → **Security policy**.
4. Click **Import**.

   This opens the standard browser window for selecting a file.
5. Specify the path to the security policy file.
6. Click the button for opening the file.

   After the file contents are checked, you will see a security policy tree showing the sections that can be imported.
7. Select the check boxes for the security policy sections that you want to import into the application.
8. Click **Import**.

The security policy import process begins. The application Server is unavailable for connections until the import process is complete. During the import process, the application web interface page displays a special section named **Application maintenance**. After the application web interface returns to its normal operating mode, re-enable use of the necessary technologies and methods.

Clearing the current security policy

You can clear the current settings that are part of a security policy. This can be done for the entire security policy or for some of its individual sections.

After a security policy is cleared, it will be impossible to recover some of its data even if you exported the security policy in advance. For example, after you clear a section containing device information, all the objects linking events and devices in the table of devices are permanently deleted.

A security policy cannot be cleared if updates are currently being installed or if the data import process is running.

Only users with the Administrator role can clear a security policy.

To clear a security policy:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface using the Administrator account.
2. Disable the use of all technologies and methods on the nodes of the Server, sensors and monitoring points.
3. Select **Settings** → **Security policy**.
4. Click **Clear**.

   You will see the security policy tree in which you can select the relevant sections to clear.
5. Select the check boxes of the security policy sections that you want to clear.
6. Click **Clear**.

   The security policy clearing process begins. The Application Server is unavailable for connections until the clearing process is complete. During the clearing process, the application web interface page displays a special section named **Application maintenance**. After the application web interface returns to its normal operating mode, re-enable use of the necessary technologies and methods.

Converting a security policy from a previous version of the application

If you want to import a file containing a saved security policy from a previous version of the application into the current version of the application, you need to convert this file by using the policy_updater.py policy conversation script. This script is located on the Server computer in the /opt/kaspersky/kics4net/sbin/ folder.

The policy_updater.py script is designed for converting security policies exported to Kaspersky Industrial CyberSecurity for Networks 3.0 and later.

To convert a file containing a security policy that was created in the previous version of the application:

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

   ```
   python3 ./policy_updater.py -i <path to the file of the original policy> -o <path to the file of the converted policy>
   ```

   Example

   ```
   python3 ./policy_updater.py -i /home/user1/policy_2025-11-01_12-00 -o /home/user1/policy_for_4_5
   ```

The obtained file can be imported into the current version of the application.

Using the Kaspersky Industrial CyberSecurity for Networks API

Kaspersky Industrial CyberSecurity for Networks has an application programming interface (API) that provides access to application functions for external applications (hereinafter referred to as "recipient applications").

The Kaspersky Industrial CyberSecurity for Networks distribution kit includes a package containing descriptions of specifications for representing data in requests sent to the REST API server. The *REST API server* runs on the Kaspersky Industrial CyberSecurity for Networks Server computer and processes requests by using the architectural style of interaction known as REST (Representational State Transfer). Queries to the REST API server are sent over the HTTPS protocol. You can configure the REST API server settings under **Settings** → **Connection servers** (including to replace the default self-signed certificate with a trusted certificate).

The JSON format is used to represent data in requests and responses.

The documentation containing descriptions of requests based on the REST architectural style is published as an Online Help Guide on the Kaspersky Online Help page. This documentation serves as the Developer Guide. The Developer Guide also provides sample code and detailed descriptions of called elements that are available in requests sent to the REST API server.

OPEN THE DOCUMENTATION DESCRIBING REQUESTS TO THE REST API SERVER, version 3

OPEN THE DOCUMENTATION DESCRIBING REQUESTS TO THE REST API SERVER, version 4

Recipient applications can use the Kaspersky Industrial CyberSecurity for Networks API to do the following:

- Receive data on devices known to the application.
- Add, modify, and delete devices.
- Receive data on registered events.
- Send events to Kaspersky Industrial CyberSecurity for Networks (the system event type with code 4000005400 is used for registering the events).
- Receive data on tags and tag parameters.
- Subscribe to notifications about received tag values.
- Receive data on detected vulnerabilities.
- Receive application messages and audit entries.
- Receive data on allow rules.
- Enable, disable, and delete allow rules.
- Receive data on risks associated with devices.
- Receive data on address spaces.

- Send a report on the network topology map to Kaspersky Industrial CyberSecurity for Networks.
- Send, receive, and delete information about users on devices.
- Send and receive information about applications and patches on devices.
- Send and delete information about executable files on devices.
- Send the contents of the device logs.
- Receive the following application data:
  - List of nodes that have application components installed
  - List of monitoring points and their parameters
  - List of supported protocol stacks and their parameters
  - List of event types and their parameters
  - Current state and operating mode of technologies
  - Application version and release dates of the installed updates
  - Information about an added license key
  - Application localization language

All of the listed actions are available when making requests to the REST API server version 4. Some of these actions are not supported when making requests to the REST API server version 3.

Recipient applications that utilize the Kaspersky Industrial CyberSecurity for Networks API can connect to the Application Server through connectors. Connectors use certificates for a secure connection. For each recipient application that will send requests to the REST API server, you need to create a separate connector in Kaspersky Industrial CyberSecurity for Networks.

A recipient application must use an authentication token for a connection with Kaspersky Industrial CyberSecurity for Networks. The application issues an authentication token upon request by the recipient application, and for this token it uses certificates of the connector that was created for this recipient application. The authentication token remains valid for 10 hours. The recipient application can renew the authentication token by special request.

Documentation containing a description of queries for authentication token operations is published as an Online Help Guide on the Kaspersky Online Help page. This documentation serves as the Developer Guide.

OPEN THE DOCUMENTATION DESCRIBING QUERIES FOR AUTHENTICATION TOKEN OPERATIONS, version 3

OPEN THE DOCUMENTATION DESCRIBING QUERIES FOR AUTHENTICATION TOKEN OPERATIONS, version 4

The Kaspersky Industrial CyberSecurity for Networks API provides the following options for working with recipient applications:

- Interaction based on the REST architectural style
- Interaction over the WebSocket protocol

Recipient applications can use the WebSocket protocol for interaction in the Kaspersky Industrial CyberSecurity for Networks API to create subscriptions to modified values received by the application. For example, this method of interaction lets you subscribe to notifications about the received values of a specific tag.

Securing interactions when using the Kaspersky Industrial CyberSecurity for Networks API

Recipient applications obtain access to application functions by using the Kaspersky Industrial CyberSecurity for Networks API after establishing encrypted connections over the HTTPS protocol. Connections are secured by using certificates issued by the Kaspersky Industrial CyberSecurity for Networks Server. The Server issues certificates for the connectors that are used by recipient applications to connect to the Server.

A separate certificate must be created for each recipient application. A connection can be established through a connector only by using the specific certificate that was issued by the Server and saved in the communication data package for that connector. A connection cannot be established if a recipient application uses a certificate from a different connector or different Kaspersky Industrial CyberSecurity for Networks Server, or a certificate that is used for other connections (such as a sensor certificate).

After establishing an encrypted connection, the recipient application must request an *authentication token* for the connector that will be indicated by the recipient application in requests sent to the REST API server. Before issuing an authentication token, the Server verifies the current state of the application user account that was indicated when the connector was created. The Server will not issue an authentication token if the application user account has been deleted or blocked.

The authentication token is valid for 10 hours after being issued by the Server. If a token needs to be used for a longer period, the recipient application must request a time extension before the token expires.

> For information on the requests and methods provided in the Kaspersky Industrial CyberSecurity for Networks Server API, please refer to the documentation for the Kaspersky Industrial CyberSecurity for Networks API.

When the Server receives requests from the recipient application during the validity period of the authentication token, the Server verifies the existence and current access rights of the application user account that was indicated when the connector was created. A method indicated in a request from a recipient application is not executed if the user account is not found (has been deleted from the application), or if the user account does not have sufficient rights to perform the operation (the user account role does not match the performed operation).

When processing requests from recipient applications, the application uses the audit log to store information about attempts to perform the following operations:

- Receive an authentication token.
- Extend the validity period for an authentication token.
- Add a device to the table of devices.

- Edit device information.
- Delete a device.
- Query the audit log (when first reading audit entries through the connector after loading the web server).

Creating and using connectors for the Kaspersky Industrial CyberSecurity for Networks API

To enable a recipient application to interact with the application by using the Kaspersky Industrial CyberSecurity for Networks API, you need to add a connector for this application. When creating a connector, you must indicate the **Generic** system type for the connector.

When adding a connector and when creating a new communication data package for this connector, the Server generates a communication data package that you need to use for the connector to work.

A communication data package is an archive containing the following files:

- certificates.pfx – encrypted file containing the Server's public certificate key and the certificate issued by the Server for the connector (with the private key). The contents of the file are encrypted with the password that was set when the connector was added or when a new communication data package was created for this connector.
- metadata.json – contains the configuration data for the connector. Data is represented in JSON format.

The listed files must be used to connect a recipient application through the connector. To decrypt the certificates.pfx file and apply the certificate and keys within it, you can use the standard methods for handling files of this format (for example, `openssl` commands). The addresses indicated in the metadata.json file are required for the connector to work and for sending requests to the REST API server.

The certificate and configuration data in the communication data package are valid until a new communication data package is created or until the connector is removed from the application.

Subscribing to notifications about tag values over the WebSocket protocol

When using the Kaspersky Industrial CyberSecurity for Networks API, a recipient application can create a subscription to notifications regarding modified values of a specific tag. The WebSocket protocol is used for creating a subscription and receiving notifications.

A subscription for a recipient application consists of the following steps:

1. **The recipient application establishes a connection with the Kaspersky Industrial CyberSecurity for Networks Server through the connector for this application using the REST API server.**

   After successfully connecting to the Server, the connector receives an authentication token. The connector uses the authentication token for all subsequent interactions with the Server in this session (specifically, for requesting its configuration from the Server).

2. **The recipient application uses WebSocket to connect and sends a request to create a subscription to notifications regarding the received values of a relevant tag.**

   The Kaspersky Industrial CyberSecurity for Networks Server receives the request and creates the subscription. A request is sent by using the appropriate functions provided by the WebSocket protocol.

3. **Kaspersky Industrial CyberSecurity for Networks detects a new tag value in traffic when reading or writing a tag.**

4. **Kaspersky Industrial CyberSecurity for Networks sends the obtained tag value to the recipient application that has an active subscription to notifications regarding the values of this tag.**

Main features of a subscription:

- After the recipient application indicates the relevant tags of Kaspersky Industrial CyberSecurity for Networks, the Server sends confirmation regarding the capability to obtain the values of those tags. The recipient application then waits to receive the values of those tags over the established connection.
- Creation and maintenance of a subscription relies on the WebSocket protocol and a connection at the same address that is used by the REST API server.
- A Kaspersky Industrial CyberSecurity for Networks Server supports no more than one active subscription for tag values. If an active subscription was already created and is being used, and you attempt to create another subscription, you will see an error regarding an excessive number of connections.
- The recipient application has the capability to close an established connection for a subscription at any time to stop receiving tag values.
- A subscription is stopped if it is intentionally closed by the recipient application or if the connection is disrupted. If the Kaspersky Industrial CyberSecurity for Networks Server was temporarily unavailable (disconnected) and tag values were not forwarded for the subscription, the recipient application must re-subscribe to the tag values after the connection is restored.

Connecting with WebSocket

To receive tags by subscription, you can use the standard functions of WebSocket as well as the SignalR Core library. Packages for working with the SignalR Core library are available for the most common programming languages: C++, C#, Java, Python, Go, and JavaScript/TypeScript.

To connect via WebSocket, you need to specify the following address:

```
<publicApi address from the communication data package>/kics4net/api/v4/tag-values
```

However, the protocol indicated in the address string depends on the functionality utilized for the connection.

If the SignalR Core library is being used, the address string begins with `https://`. For example:

```
https://kics-server:8080/kics4net/api/v4/tag-values
```

If the standard functions of WebSocket are being used, you need to replace `https` with `wss` in the address string. For example:

```
wss://kics-server:8080/kics4net/api/v4/tag-values
```

If an authentication token is not provided when connecting (or the provided token has not passed verification), the server returns code 401 when responding to a request to open the connection.

Creating a subscription for tag values

To create a subscription, you must make a request with the `GetTagValuesStream` method name.

Example request argument

```
{
 "tagIdentifiers": [
 { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
 { "tagName": "Asdu_1_object_1003", "assetName": "Asset 079" }
 ],
 "streamConfig": {
 "samplingRateHz": 1
 }
}
```

A request argument consists of the following fields:

- `tagIdentifiers` – array of IDs of tags whose values need to be received for the subscription.
- `assetName`, `tagName` – values representing the device name and tag name (used to identify the tag whose values are needed for the subscription).
- `samplingRateHz` – tag value sampling rate (used to reduce the volume of transmitted data). If a null value is defined for the field, sampling is not performed.

If a subscription creation argument does not satisfy the requirements of the fields, an error is returned with a description of the problem.

Example error for a subscription creation argument

```
HubException: GetTagValuesStreamRequest has validation errors:
 TagIdentifiers:
 The TagName field is required.
 The StreamConfig field is required.
```

Confirming a subscription

When confirming a subscription, the server returns a confirmation result for each tag that matches a `tagIdentifiers` value in the request.

Example subscription confirmation

```
{
 "confirmation": {
 "result": "ok",
 "tagIdentifier": { "tagName": "Asdu_1_object_1001", "assetName": "Asset 079" },
 "tagId": 102
 }
}
```

A response containing a subscription confirmation consists of the following fields:

- `result` – status of the tag value subscription. Possible values:
  - `ok` – subscription was successfully created.
  - `notFound` – a tag with the specified `assetName` or `tagName` was not found.
- `tagIdentifier` – tag ID equivalent to one value from the `tagIdentifiers` array of arguments of a subscription creation request.
- `tagId` – unique ID of a tag in the application. This can be used to receive information about a tag through the Kaspersky Industrial CyberSecurity for Networks API, or to identify a tag in a response containing its values.

Tag values by subscription

The application sends tag values by subscription within a fields structure. The following fields are presented at the top level of the structure:

```
{
 "value": {
 "tagId": <unique ID of the tag in the application>
 "tagValue": "<JSON object containing tag data>"
 }
}
```

Information about a new value of a tag is sent to the recipient application in JSON format. The sent data object contains the following fields:

- `n` – tag data type represented by the name from `TagStructure`.
- `ts` – time when the last update of tag values was registered. Indicated in microseconds starting on 01/01/1970.
- `dn` – transfer direction. Possible values: `r`, `w`, `rw`.

- `mp` – monitoring point ID.
- `d` – contents of tag fields.

The `d` attribute represents a dictionary in which each key is the name of a null-hierarchy tag field. Each field value has the following attributes:

- `t` – mandatory attribute indicating one of the following data types:
  - `u` – UINT64
  - `i` – INT64
  - `b` – BOOL
  - `d` – DOUBLE
  - `s` – UTF8 string
  - `t` – time in microseconds starting on 01/01/1970
  - `e` – ENUM The field additionally contains the following attributes:
    - `n` – name of the ENUM type
    - `v` – original value of ENUM
    - `s` – string value of ENUM
  - `st` – structure
  - `un` – UNION
- `v` – mandatory attribute indicating the tag field value
- `n` – name of the ENUM type from `TagStructure` (only for the `e` type – ENUM)
- `s` – string value of ENUM (only for the `e` type – ENUM)

  Example

  ```
  - enum:
   name: OpType # Name of the ENUM type ('n' attribute)
   data:
   0: NUL # 0 is written to the 'v' attribute, NUL is written to the 's' attribute
   1: PULSE_ON
   2: PULSE_OFF
  ```

- `x` – identifies the main value of the tag.

  Format: `"x": 1`

  The `x` attribute is absent from all other fields of the tag.

- `m` – special marker of the tag parameter. This corresponds to the `marker` attribute with the following fields:
  - `q` – value of the quality attribute.
  - `ts` – timestamp status displaying its accuracy, temporary state, or reason for an error during verification.
  - `ds` – data status.
  - `o` – origin of the value or command.
  - `t` – time when the tag values were last updated (taken from traffic).
  - `ct` – cause of transmission.

  Format: `"m": "q"`

Example of a forwarded tag value in JSON format


```
{
 "n": "TagStructure1",
 "ts": 1784035816,
 "dn": "r",
 "mp": 1,
 "d":
 {
 "value":
 {
 "t": "d",
 "v": 3.1415,
 "x": 1
 },
 "quality":
 {
 "t": "s",
 "v": "good",
 "m": "q"
 },
 "mask":
 {
 "t": "u",
 "v": 1784035816
 },
 "enumfield":
 {
 "t": "e",
 "n": "SwitchState",
 "v": 0,
 "s": "Off"
 },
 "strucfield":
 {
 "t": "st",
 "v":
 {
 "v1":
 {
 "t": "d",
 "v": 3.1415
 },
 "q2":
 {
 "t": "s",
 "v": "good",
 "m": "q"
 }
 }
 },
 "unionfield":
 {
 "t": "un",
 "v":
 {
 "_":
 {
```

```
 "t": "u",
 "v": 42
 },
 "low4bits":
 {
 "t": "u",
 "v": 10
 },
 "high4bits":
 {
 "t": "u",
 "v": 2
 }
 }
 }
 }
}
```

Examples of receiving tag values by subscription

Below is an example of receiving tag values by subscription using standard WebSocket functions in Python.

You must first run the following command:

```
pip install websocket_client
```

Example subscription using standard WebSocket functions

```
import json, ssl, websocket


def on_message(ws, message):
 print(message)


def on_error(ws, error):
 print(f' error: {error}')


def on_close(ws):
 print("### closed ###")


def on_open(ws):
 print("connection opened and handshake received ready to send messages")

 # all sent messages must end with this character
 message_separator = chr(30)

 # setting up json as messages format
 protocol_selection_args = {
 'protocol': 'json',
 'version': 1
 }
 ws.send(json.dumps(protocol_selection_args) + message_separator)

 # creating subscription
 args = {
 'arguments': [
 {
 'tagIdentifiers': [
 {
 'tagName': 'tag_01',
 'assetName': 'asset_02'
 }
 ],
 'streamConfig': {
 'samplingRateHz': 5
 }
 }
```

```
],
'invocationId': '0', # will be included in response message
'target': 'getTagValuesStream',
'type': 4 # must be equal to 4 for outgoing messages
}

ws.send(json.dumps(args) + message_separator)


def login():
token = "you should get access token for API here"
return token


if __name__ == "__main__":
server_url = "wss://localhost:8091/kics4net/api/v4/tag-values"
auth = "Authorization: Bearer " + login()

# for troubleshooting uncomment next line
# websocket.enableTrace(True)
ws = websocket.WebSocketApp(server_url,
on_message=on_message,
on_error=on_error,
on_close=on_close,
header=[auth])

print(f'opening connection to {server_url}')
ws.on_open = on_open
ws.run_forever(
# use it only if Server has self-signed certificate
sslopt={"cert_reqs": ssl.CERT_NONE}
)
```

Below is an example of receiving tag values by subscription using the SignalR Core library in Python.

You must first run the following command:

```
pip install signalrcore
```

Example subscription using the SignalR Core library

```
import logging
from signalrcore.hub_connection_builder import HubConnectionBuilder

TOKEN = 'you should get access token for API here'
IP = '192.168.2.7'
PORT = '8080'
HUB = 'kics4net/api/v4/tag-values'

class WebsocketConnection(HubConnectionBuilder):
def __init__(self, url: str = None, options: dict = None, verify_ssl: bool = False):
super().__init__()
self.with_url(url, options=options)
self.configure_logging(logging.WARNING)
self.with_automatic_reconnect({
"type": "raw",
"keep_alive_interval": 10,
"reconnect_interval": 5,
"max_attempts": 5
})
self.verify_ssl = verify_ssl

def on_tag_stream_value(self, m):
result.append(m)
print(f'on_new_tag_value, {m}')

def on_tag_strean_error(self, e):
print(f'onError, {e}')

def on_tag_stream_complete(self, q):
print(f'onComplete, {q}')

def subscribe_tags(self):
print("connection opened and handshake received ready to send messages")

args = {
'tagIdentifiers': [
```

```
  {
  'tagName': 'tag_01',
  'assetName': 'asset_02'}
  ],
  'streamConfig': {
  'samplingRateHz': 5
  }
  }

  self.stream("GetTagValuesStream", [args]) \
  .subscribe({
  "next": self.on_tag_stream_value,
  "complete": self.on_tag_stream_complete,
  "error": self.on_tag_strean_error
  })

def main():
  server_url = "https://{}:{}/{}".format(IP, PORT, HUB)
  login = 'bearer {}'.format(TOKEN)

  conn = WebsocketConnection(url=server_url, options={"headers": {"authorization": login}})
  conn.build()

  logging.info(f'opening connection to {server_url}')
  conn.on_open(conn.subscribe_tags)
  conn.start()

  logging.info('closing connection')
  conn.stop()


if __name__ == '__main__':
  main()
```

Performing common tasks

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

System monitoring in online mode

Kaspersky Industrial CyberSecurity for Networks displays data for monitoring the current state of the system in the **Dashboard** section of the application web interface. Data is automatically updated in online mode.

Data in the **Dashboard** section is presented as individual blocks called *widgets*. Depending on its purpose, a widget may contain an updatable value or message about the current state of the application, or provide expanded information about up-to-date data.

The **Dashboard** section may display the following widgets:

- Widgets containing information for monitoring the current state of the system and the most significant changes:
  - **Devices with security states** (in Kaspersky Industrial CyberSecurity for Networks 4.5.1, the widget is called **Device security statuses**) – distribution of devices by their security states.
  - **Event scores** – histogram that arranges events based on their scores for the selected period. Columns of the histogram correspond to integer values of event scores. You can change how data is displayed on the pie chart that arranges events by their severity level. Depending on its score, an event may have a severity of *Low* (score of 0.0–3.9), *Medium* (4.0–7.9), or *High* (8.0–10.0).
  - **Events by technology** (in Kaspersky Industrial CyberSecurity for Networks 4.5.1, the widget is called **Event technologies**) – quantitative distribution of events by event registration technologies for the selected period.
  - **Frequently encountered users of applications in events** – shows the most frequently registered user names in events based on data from EPP applications for the selected period.
  - **Frequently encountered applications in events** – shows the most frequently registered recipient applications in events based on data from EPP applications for the selected period.
  - **Frequently encountered devices in events** – shows the most frequently registered devices in events for the selected period.
  - **Top devices by risk count** – shows the most frequently registered devices in detected risks for the selected period.
  - **Risk scores** – histogram that arranges risks based on their scores for the selected period. Columns of the histogram correspond to integer values of event scores. You can change how data is displayed on the pie chart that arranges risks by their severity level. Depending on its score, a risk may have a severity of *Low* (score of 0.0–3.9), *Medium* (4.0–7.9), or *High* (8.0–10.0).
  - **Device statuses** (available only in Kaspersky Industrial CyberSecurity for Networks 4.5.1) – distribution of devices by their statuses.
  - **Devices** – contains information about devices on the industrial network (arranged by device category).

- **Events** – contains information about the events and incidents that have the most recent values for the date and time of last occurrence.

- **Situational awareness** – shows notifications about currently identified threats to system security (for example, **Detected 10 unauthorized network interactions**). This widget displays notifications in the order of their severity.

- **Protection by EPP applications** – quantitative ratio of computers protected by EPP applications to computers not protected by EPP applications. The total quantity is displayed in the center of the pie chart. Devices that meet certain conditions are counted as protected and unprotected computers in the widget.

- **Traffic by protocols** (available only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1) – distribution of traffic over detected protocols for the selected period. The widget displays a graph of traffic volume for the protocols selected in the right part of the widget. The protocols are shown in the graph as separate layers filled with the corresponding colors. When selecting protocols in the right part of the widget, no more than 14 different protocols are available (protocols with a non-zero traffic volume that are not included in the main list on the widget are represented by the additional general element **Other protocols**). If you want the widget to display data only for certain protocols, you can select these protocols when changing the data display settings in the widget.

- Widgets containing information about the application and about the hardware resources of the Server and sensors:

  - **Traffic** – rate of incoming traffic. This widget can display data on all monitoring points of all nodes that have application components installed, data on monitoring points of the selected node, or data on one individual monitoring point.

  - **CPU** – processor utilization on the selected node that has an application component installed.

  - **RAM** – amount of physical RAM being used on the selected node that has an application component installed.

  - **Performance** – information about the current state of application performance. This widget can display the following values:

    - **OK** – there are no messages regarding performance issues, or all performance issues have been resolved.

    - **Non-critical malfunction** – there are messages regarding non-critical malfunctions (this is displayed until the performance issue is resolved).

    - **Operation disrupted** – there are messages regarding application performance issues (this is displayed until the performance issue is resolved).

    - **Maintenance mode** – the application is running in maintenance mode.

  - **Tags** – rate of processing of the tags detected by the application. This widget can display data on all monitoring points of all nodes that have application components installed, data on monitoring points of the selected node, or data on one individual monitoring point.

  - **Storage** – information about the drive in the local file system on the selected node with the application component installed. On this widget, you can select the following data to be displayed:

    - **Disk usage** – percentage of time taken to process data read/write operations.

    - **Occupied on disk** – volume of used disk space.

- **Read from disk** – rate of reading data from the disk.
- **Write to disk** – rate of writing data to the disk.

- **Traffic processing latency** – current delay in traffic processing from the time it arrives at a monitoring point of the node (displays the maximum delay time received from all enabled monitoring points). This widget can display data on all monitoring points of all nodes that have application components installed, or data on monitoring points of the selected node.

- **Status of functions** – general information about the current state of protection functions in the application. This widget can display the following values:
  - **All are enabled** – all technologies and methods designed for continual use are enabled, and all created monitoring points are enabled.
  - **Not all are enabled** – some protection functions are disabled or are enabled in learning mode, or not all monitoring points are enabled.

- **Uptime** – Kaspersky Industrial CyberSecurity for Networks running time. On this widget, you can select the following data to be displayed:
  - **Effective uptime** – duration of normal operation of the application (without malfunctions) since the most recent startup until the current moment.
  - **Total uptime** – total running time since the first startup of the application until the current time (includes periods of normal operation and periods when the application was running with malfunctions).
  - **Since first start of application** (in Kaspersky Industrial CyberSecurity for Networks version 4.5.1, this setting is named **Time since first run**) – the total time elapsed from the first startup of the application to the current time (includes periods of normal operation of the application, periods of malfunctions, and periods of inoperability).

- Widgets without dynamically updated information. You can create widgets with user-defined contents. These widgets are called *custom* widgets. For example, you can use custom widgets to logically separate groups of widgets in the **Dashboard** section.

Widgets provide various ways to get your attention depending on incoming data. For example, widgets containing information about the application and hardware resources can automatically change color if the information requires attention (for instance, when the load on a hardware resource is nearing critical load).

Widgets display only the main information, which is dynamically updated. If you need to view more detailed information (for example, about devices with issues), you can proceed from the **Dashboard** section to other sections of the application web interface. You can switch between sections by using your mouse to select interface elements of widgets.

Adding a widget

To add a widget:

1. In the **Dashboard** section, click **Widgets**.

   The **Add widgets** window opens.

2. Add the relevant widget by clicking **Add** on the right of the widget name.

   The new widget will occupy the free space in the widget display area.

3. Click **Close** in the **Add widgets** window.

After adding a widget, you can configure how the widget is displayed.

Configuring how widgets are displayed

This section provides instructions on customizing widget display.

Moving a widget

To move a widget:

1. In the **Dashboard** section, move your cursor over the upper part of the relevant widget (for example, over the widget name).

   The cursor will change to .

2. Drag the widget to the appropriate part of the widget display area.

Changing the size of a widget

To resize a widget:

1. In the **Dashboard** section, move your cursor over the lower-right corner of the relevant widget.
2. Click and hold the left mouse button to set the size for the widget border.

Changing the settings for displaying data in a widget

After a widget is added, the default settings are used to display data in the widget. You can change the display settings if necessary (for example, to indicate the relevant source or to select other data to display in the **Storage** widget).

To configure the widget display settings:

1. In the **Dashboard** section, click ⚙ in the upper-right corner of the widget to open the widget management window.
2. In the widget management menu, select **Configure**.

   This opens the window for configuring the display settings.

3. Configure the widget settings.

Depending on the selected widget, the window may contain the following settings:

- **Change name** – if the **Change name** check box is selected, you can define any name for the widget (different from the default name) in the **Widget name** field. The **Change name** setting is absent from custom widgets.
- **Widget name** – field for entering a widget name different from the default name.
- **Change description** – if the **Change description** check box is selected, you can provide any description for the widget (different from the default description) in the **Widget description** field. The **Change description** setting is absent from custom widgets.
- **Widget description** – field for entering a widget description different from the default description.
- **Refresh period (sec)** – defines how frequently the displayed data is refreshed (time interval in seconds).
- **Protocols** – specifies the protocols whose data should be displayed in the widget. You can select the necessary protocols in the same way as when filtering data tables by the **Protocol** column.
- **Show** – defines the type of displayed data (for widgets that let you select which data to display).
- **Data source** – defines the node with installed application components whose data is displayed in the widget. If **Entire application** is selected, the widget displays data from all nodes.
- **Monitoring point** – defines the monitoring point of the selected node for displaying data. If **All monitoring points** is selected, the widget displays data for all monitoring points of the selected node.
- **Change color based on status** – if this check box is selected, the background color of the widget automatically changes depending on the severity of the incoming data. A red background signifies critical (maximum) severity of data. If this check box is cleared, background coloring is disabled.
- **Defined background** – defines the color of the background on the custom widget. You can choose a background color that corresponds to one of the severity levels (**Informational**, **Warning**, or **Critical**) or select **Neutral** to disable background coloring.
- **Display mode** – determines how data is displayed in the widget. You can configure the widget to display data as a histogram or pie chart.
- **Take into account events with Resolved status** – if **Take into account events with Resolved status** is selected, the widget displays data for all events.
- **Include remediated and accepted risks** – if **Include remediated and accepted risks** is selected, the widget displays data for all risks.

4. Click **OK**.

Information in the Devices widget

The **Devices** widget in the **Dashboard** section displays information about devices that are included in the list of known devices.

The widget provides the following information:

- Data on the number of devices known to the application in each category. This data is displayed as category icons in the upper part of the widget. The number of devices of the specific category is indicated under the icon of each category. If the list of devices contains devices with issues, the warning icon is displayed on the category icons of these devices.
- List of categories with devices with issues. This data is displayed in the middle part of the widget if such devices are present. The space used for displaying graphical elements is limited by the size of the widget.

Devices with issues

The application determines that a device requires attention in any of the following cases:

- The device has a status of *Authorized* and a security state other than *OK*.
- The device has a status of *Unauthorized*.

If there are devices with issues, the following information is displayed for each category in the list:

- Line containing the category icon, text comment, and link containing the number of devices with issues.
- Line containing the graphical elements representing the devices. This line is displayed if there is sufficient free space in the widget. The number of graphical elements in the line depends on the current size of the browser window. If there are more devices with issues than the number of graphical elements displayed in the line, the number of hidden devices is displayed on the right in the format `+<number of devices>`.

Graphical elements of devices

Graphical elements representing devices contain the following information:

- Device name.
- Device status. This is displayed as an icon if the device has a status of *Unauthorized*.
- Device security state. This is displayed as a colored line on the left border of the graphical element. The color of the line corresponds to the *OK*, *Warning*, or *Critical* states.

The graphical elements are displayed in the following order:

1. Devices assigned a status of *Unauthorized*.
2. Devices with a *Critical* security state.
3. Devices with a *Warning* security state.

Navigating to other sections from the widget

You can use elements of the **Devices** widget interface to navigate to the table of devices and display detailed information about devices. The following options are available to achieve this.

Go to the table of devices and filter the table

To go to the table of devices and view information about all devices in the selected category:

In the upper part of the **Devices** widget, click the icon of the relevant category.

This opens the **Assets** section containing the table of devices. The table will be filtered based on the selected category of devices.

To proceed to the table of devices and view information about devices with issues that belong to a specific category:

In the list of categories containing devices with issues, click the link displaying the number of devices in the relevant category. This link is displayed at the end of the line with the category icon and text comment **with issues**.

This opens the **Assets** section containing the table of devices. The table will be filtered based on the IDs of devices with issues that belong to the specific category.

The table of devices is filtered based on the IDs of those devices that were displayed in the **Devices** widget when you proceeded to the table of devices. After you switch to the table of devices, the filter settings are not updated. If you want to view the current number of devices with issues, you can go to the **Dashboard** section again.

To go to the table of devices and view information about a device with issues:

In the **Devices** widget, click the graphical element that represents the relevant device.

This opens the **Assets** section containing the table of devices. The table will be filtered based on the device ID.

To go to the table of devices without changing the current table filter settings:

Click **Show all devices** in the **Devices** widget.

This opens the **Assets** section containing the table of devices. The table will display the devices that satisfy the filter settings that were previously defined in the table of devices.

Go to the table of devices and search the table

To go to the table of devices and find devices in the table:

1. In the **Devices** widget, enter your search query into the **Search devices** field.
2. Click **Search**.

   This opens the **Assets** section containing the table of devices. The table will display the devices that meet the search criteria.

Information in the Events widget

The **Events** widget in the **Dashboard** section displays general information about the events and incidents that have the most recent values for the date and time of last occurrence.

The widget displays the following elements:

- Histogram of events and incidents for the selected period. This data is displayed in the upper part of the widget. The histogram shows the distribution of events and incidents based on their severity levels.
- List containing information about registered events and incidents sorted by date and time of last occurrence. This data is displayed in the middle part of the widget.

Statistics of events and incidents

On the histogram showing the distribution of events and incidents, the columns correspond to the total number of events for each time interval. Within columns, the severities of events and incidents are distinguished by color. The following colors correspond to severity levels:

- Blue. This color is used for events and incidents with a *Low* severity level.
- Yellow. This color is used for events and incidents with a *Medium* severity level.
- Red. This color is used for events and incidents with a *High* severity level.

To display information about a column of the histogram, move the mouse cursor over it. A pop-up window shows the date and time of the interval as well as the number of events and incidents by severity level.

The duration of time intervals depends on the selected display period. You can select the relevant period for generating a histogram using the following buttons:

- **1h**—period of one hour, divided into intervals of one minute.
- **12h**—period of 12 hours, divided into one-hour intervals.

- **24h**—period of 24 hours, divided into one-hour intervals.
- **7d**—period of seven days, divided into intervals of one day.

List of events and incidents

The list of events and incidents in the **Events** widget is updated in real time. Events and incidents with the most recent values for the date and time of last occurrence are placed at the beginning of the list.

The number of displayed elements in the list of events and incidents is limited by the size of the widget.

The following information is provided for each event or incident in the list:

- Title of the event or incident.
- Date and time of last occurrence.
- Icon designating the severity level of an event or incident:
  - – *Low* severity level
  - – *Medium* severity level
  - – *High* severity level

Incidents in the list are marked with the icon.

Navigating to other sections from the widget

You can use elements of the **Events** widget interface to go to the table of events and display detailed information about events and incidents. The following options are available to achieve this.

Go to the table of events and filter the table

You can view detailed information about an event or incident by clicking the relevant event or incident in the **Events** widget list. Doing so will open the **Events** section in which the table will be filtered based on the ID of the selected event or incident. The period ranging from the date and time of registration of the event or incident to the current moment (without indicating an end boundary for the period) will also be defined for the filter.

If you want to proceed to the table of events without changing the current table filter settings in the **Events** section, click **Show all events** in the **Events** widget.

Go to the table of events and search the table

To go to the table of devices and find devices in the table:

1. In the **Events** widget, enter your search query into the **Search events** field.
2. Click **Search**.

The **Events** section opens. The table of events displays the events and incidents that meet the search criteria.

Conditions determining how devices are taken into account in the Protection by EPP applications widget

The **Protection by EPP applications** widget displays the number of devices protected by EPP applications and the number of unprotected devices that could potentially be protected by EPP applications.

A device is considered protected by an EPP application and is included in the list of **Computers with an active EPP application** if Kaspersky Industrial CyberSecurity for Networks has information about the fulfillment of all the following conditions:

- An EPP application is installed on the computer and this application has been configured to work with Kaspersky Industrial CyberSecurity for Networks.
- The Real-Time Protection task is being performed for the EPP application.
- The EPP application has an *Active* connection to the integration server.
- The device has been assigned any status except the *Archived* status (taken into account only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).

A device is considered unprotected by an EPP application and is included in the **Computers without EPP applications** list if this device is not included in the list of devices protected by EPP applications, the device is not assigned the *Archived* status, and one of the following conditions is also fulfilled:

- The device belongs to one of the following categories:
  - **Server**
  - **Workstation**
  - **HMI / SCADA** (taken into account only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1)
  - **Engineering workstation** (taken into account only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1)
- The EPP application sent information from this device to the integration server (taken into account only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).
- The device information indicates the name of any version of a Windows operating system as the installed operating system (it is not taken into account in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).

Removing a widget

To remove a widget:

1. In the **Dashboard** section, click ⚙ in the upper-right corner of the widget to open the widget management window.
2. In the widget management menu, select **Delete**.

   A window with a confirmation prompt opens.
3. In the prompt window, confirm removal of the selected widget.

Asset Management

Kaspersky Industrial CyberSecurity for Networks lets you monitor industrial network devices that are considered to be company assets. To manage these assets, you can view the table of devices in the **Assets** section of the Kaspersky Industrial CyberSecurity for Networks web interface. You can also view information about the interactions between devices and perform various actions with devices when working with the network interaction map and with the topology map.

Table of devices

A table of devices is created for the purpose of asset management in the application. All devices in the table are considered to be known to the application. You can view the table of devices in the **Assets** section on the **Devices** tab.

The table of devices has the following limitations on the number of elements:

- The total number of devices with a status of *Authorized* or *Unauthorized* can be no more than 100 thousand.

  If the maximum number of devices with a status of *Authorized* or *Unauthorized* is reached, new devices with these statuses are not added to the table. If this is the case, to add a new device to the table you need to remove one of the previously added devices.

- The number of devices with a status of *Archived* can be no more than 100 thousand.

  If the maximum number of devices with the *Archived* status is reached, new devices with this status are added to the table in place of devices that have went the longest without showing any activity.

When the table of devices is overfilled, the application displays the appropriate message.

The table of devices contains the following information:

- **Name** – name that represents the device in the application.
- **Device ID** – device ID assigned in Kaspersky Industrial CyberSecurity for Networks.

- **Status** – asset status that determines whether activity of the device is allowed in the industrial network. A device can have one of the following statuses:
  - *Authorized*. This status is assigned to a device for which activity is allowed in the industrial network.
  - *Unauthorized*. This status is assigned to a device for which activity is not allowed in the industrial network.
  - *Archived*. This status is assigned to a device if it is no longer being used or must not be used in the industrial network, or if the device has shown no activity and the device information has not changed in a long time (30 days or more).
- **Address information** – device MAC and/or IP address. If a device has multiple network interfaces, you can specify different MAC- and/or IP addresses for the device on different network interfaces (up to 512 network interfaces can be indicated in the device information). If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the table of devices. When you view information about a device, the information about the MAC and/or IP address of the device and address spaces are displayed on the **Addresses** tab.
- **Category** – name of the category that determines the functional purpose of the device. Kaspersky Industrial CyberSecurity for Networks supports the following categories of devices:
  - **PLC** – programmable logic controllers.
  - **IED** – intelligent electronic devices.
  - **HMI / SCADA** – computers with installed software for human-machine interface (HMI) systems or SCADA systems.
  - **Engineering workstation** – computers with installed software to be used by ICS engineers.
  - **Server** – devices with server software installed.
  - **Network device** – network equipment (for example, routers or switches).
  - **Workstation** – desktop personal computers or operator workstations.
  - **Mobile device** – portable electronic devices with computer functionality.
  - **Laptop** – portable PCs.
  - **HMI panel** – devices that use a human-machine interface to manage individual devices or operations of the industrial process.
  - **Printer** – printing devices.
  - **UPS** – uninterruptible power supply units connected to a computer network.
  - **Network camera** – devices that perform video surveillance functions and transmit digital images.
  - **Gateway** – devices that connect networks by converting various interfaces (for example, Serial/Ethernet) within networks that use a different data transfer medium and different protocols.
  - **Storage system** – devices used for storing information in storage systems.
  - **Firewall** – devices that perform firewall functions to inspect and block unwanted traffic.

- **Switch** – devices used for a physical connection between LAN nodes.
- **Virtual switch** – devices that logically merge physical switches, or software-implemented switches for virtualization systems.
- **Router** – devices that redirect network packets between segments of a computer network.
- **Virtual router** – devices that logically merge physical routers, or routers that utilize multiple independent routing tables.
- **Wi-Fi** – access points that provide a wireless connection for devices from Wi-Fi networks.
- **Historian server** – archive data servers.
- **Other** – devices that do not fall into the categories described above.

- **Group** – name of the group containing the device in the device group tree (contains the name of the group and the names of all its parent groups).
- **Security state** – device security state determined by the presence of events linked to the device. The following security states are available:
  - *Critical*. Events associated with the device have severity rating 8.0–10.0.
  - *Warning*. Events associated with the device have severity rating 4.0–7.9.
  - *OK* Events associated with the device have severity rating 0.0–3.9, or the device has no associated events.
- **Importance** – importance of the device to the enterprise. Importance is assigned to a device based on its category. The following device importance levels are provided:
  - *High*. Assigned to the devices of the following categories: **PLC**, **IED**, **HMI / SCADA**, or **Server**.
  - *Medium*. Assigned to the devices of the following categories: **Engineering workstation**, **Network device**, **Workstation**, **HMI panel**, **Gateway**, **Storage system**, **Firewall**, **Switch**, **Virtual switch**, **Router**, **Virtual router**, **Wi-Fi**, or **Historian server**.
  - *Low*. Assigned to the devices of the following categories: **Mobile device**, **Laptop**, **Printer**, **UPS**, **Network camera**, or **Other**.
- **Last seen** – date and time when the last activity of the device was registered.
- **Risks** – risk categories detected for the device. By default, the table of devices displays information for current risks only. To display information on all risks, select the **Show remediated and accepted risks** check box when configuring the table of devices.
- **Last modified** – date and time when information about the device was last modified.
- **Created** – date and time when the device was added to the table of devices.
- **OS** – name of the operating system installed on the device.
- **Hardware vendor** – name of the device hardware vendor. In the details area, this setting is referred to as **Vendor** and is displayed on the **General** tab in the **Hardware** settings group.

- **Hardware model** – device model name. In the details area, this setting is referred to as **Model** and is displayed on the **General** tab in the **Hardware** settings group.
- **Hardware version** – device hardware version number. In the details area, this setting is referred to as **Version** and is displayed on the **General** tab in the **Hardware** settings group.
- **Software vendor** – name of the device software vendor. In the details area, this setting is referred to as **Vendor** and is displayed on the **General** tab in the **Software** settings group.
- **Software name** – name of the device software. In the details area, this setting is referred to as **Name** and is displayed on the **General** tab in the **Software** settings group.
- **Software version** – device software version number. In the details area, this setting is referred to as **Version** and is displayed on the **General** tab in the **Software** settings group.
- **Network name** – name used to represent the device in the network.
- **Labels** – list of labels assigned to a device.
- **Process Control settings** – indicator of whether there are Process Control settings defined for the device. In the details area, the Process Control settings configured for the device are displayed on the **Process control** tab.
- **EPP application** – concise name of the EPP application installed on the device (if data from this application was received in Kaspersky Industrial CyberSecurity for Networks).
- **EPP connection** – status of the connection between the integration server and the EPP application installed on the device. The following statuses are available:
  - *Active*. Less than 24 hours have passed since the last connection between the application and the integration server.
  - *Inactive*. More than 24 hours have passed since the last connection between the program and the integration server.
  - *N/A*. The status of the connection is unknown.
- **Last connection to EPP** – date of the last connection between the integration server and the EPP application installed on the device.

When viewing the table of devices, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing device information

Detailed information about a device includes information from the table of devices, and the following fields (if values are available for these fields):

- **Router** – indicator of a routing device.

  If the router indicator is not determined automatically, it must be set manually, for example, for a device that performs the functions of a network switch between the industrial network segments. This attribute allows the application to use additional algorithms for detecting devices that interact with each other through a router. In particular, if the router indicator is set, either automatically or manually, for a network switch that connects a segment with several PLCs and a computer segment with a SCADA system, the application is able to detect and add to the table of devices all new devices in the first segment that interact with a computer with the SCADA system in the second segment.

- **Additional information** – additional information about a device specified by an application user (for example, a description of the device deployment location).

- **Custom fields** – set of non-standard device information defined by an application user (for example, categories and classes of device protection). Up to 16 custom fields may be specified for a device.

- **Dynamic fields** – set of expanded device information detected in traffic when the device information detection method is being employed. This field is displayed if expanded information was detected by the application.

- **Endpoint Agent** – information about the Endpoint Agent software component on the device.

- A **Public key** is a saved value for device verification before establishing an SSH connection and scanning the device as part of security audit jobs.

- **Network behavior** – tab containing information about Device Control based on network interaction rules, device training quality indicators (compliance of detected interactions with active allow rules), and device network interaction statistics.

- **Topology** – tab containing information about the last active poll of the device, as well as information about the device connections to other nodes.

- **Equipment** – tab containing information about BIOS applications and device processors, information about the amount of free RAM and memory on the device local drives, and information about the USB devices and optical drives used. The information is displayed if obtained through equipment monitoring.

- **Configurations** – tab containing information about the received device configurations. The information is displayed if obtained as a result of the configuration control jobs.

To view device information:

On the **Devices** tab in the **Assets** section, select the relevant device.

The details area appears in the right part of the web interface window. The details area displays all data that has defined values.

Automatically adding and updating devices

The application can automatically add devices to the table and update information about devices. To automatically add and update devices in Kaspersky Industrial CyberSecurity for Networks, you must enable the following asset management methods:

- Device Activity Detection. When using this method, the application adds newly detected devices to the table based on the obtained MAC- and/or IP addresses of the devices. If the application detects activity of an already known device, it may change its status depending on the current asset management mode.

- Device Information Detection. When using this method, the application updates information about known devices based on data received from traffic or from EPP applications. Based on data received from traffic, the application updates the information for which automatic updates are enabled in the device settings (this is enabled by default until an application user manually changes a value). If device information detection is disabled, the application does not update or augment available device information based on data received from traffic or from EPP applications.

When adding a device, the application assigns a device name based on the default template: **Device <value of the internal device counter>**. The value of the internal counter in the device name may differ from the device ID that is displayed in the **Device ID** column.

Using device information detection, the application can update a device name after receiving the following information:

- Device model name.

- Network name used to represent the device on the network (the network name of the device takes priority during an update).

The application can automatically update information related to the vendors of network equipment based on the MAC addresses of devices. To identify vendors based on MAC addresses, the application compares the MAC addresses of devices with the address ranges that are registered in the public database of the international Institute of Electrical and Electronics Engineers (IEEE). If a network equipment vendor is identified by MAC address, the application uses the same vendor name that is presented in the IEEE database.

After the application is installed, it uses a copy of the IEEE database containing information about MAC addresses and vendors that was up to date when the current version of the application was released. You can keep the local copy of the IEEE database up to date by installing updates.

Automatically merging devices

The application can take several devices added to the devices table and merge them into one device. Devices can be merged automatically when the Device Activity Detection method is enabled in learning mode.

Devices are automatically merged if the application identifies a link between the MAC address of one device and the IP address of a different device. Also, a link between device addresses may be established based on the results of active polling or based on data received from EPP applications. If conflicts arise between defined values in the data on merged devices, the new device will retain the values that were defined for the following devices:

- Devices with a saved IP address – if a link between the IP address and the MAC address of another device is detected.

  Prior to enabling learning mode (and while working in this mode), it is not recommended to change information about devices for which only a MAC address is defined if they could be automatically merged with devices that have defined IP addresses.

- Devices with an IP address and the Endpoint Agent software component installed – if a link to other devices is detected based on data from EPP applications.
- Devices with the most IP addresses.
- Devices with the most addresses – if all merged devices lack an IP address.

When devices are merged, some information from the merged devices might not be saved in the new device (for example, the contents of dynamic fields and topology parameters).

Automatically assigning the statuses of devices

When monitoring the activity of devices in the industrial network, the application can automatically assign statuses to detected devices based on the obtained MAC- and/or IP addresses of devices. Statuses are assigned depending on the current asset management mode.

In learning mode, the application assigns a status of *Authorized* to all detected devices (this includes new devices as well as devices that were previously added to the table of devices). If a status of *Unauthorized* was previously assigned to a detected device, its status is not changed.

In monitoring mode, the assigned status depends on whether the device that showed activity is known or unknown to the application. In this mode, statuses are assigned according to the following rules:

- If a device is new (not present in the table of devices when it is detected), a status of *Unauthorized* is assigned to it.
- If the device is in the table of devices and has a status of *Authorized* or *Unauthorized*, the status is not changed.
- If the device is in the table of devices with a status of *Archived*, a status of *Unauthorized* is assigned to this device.

By default, if a device with a status of *Authorized* has not shown any activity in over 30 days and the device information has not changed during this time, a status of *Archived* is assigned to this device. You can disable automatic device status change to *Archived* when manually changing device status (for example, to prevent *Authorized* from automatically changing to *Archived* for rarely connected devices).

Cisco Switch connectors may automatically restrict network access for devices that have a status of *Unauthorized*. To avoid blocking necessary devices due to status changes, check the settings you defined for this connector type.

When devices with a status of *Unauthorized* appear in the table of devices, you need to determine whether all of these devices are required for industrial process support. After making this determination, it is recommended to manually assign one of the following statuses to each device:

- *Authorized* – if the device is required for industrial process support.
- *Archived* – if the device should not be used in the industrial network.

  Instead of assigning a status of *Archived*, you can delete the device. However, all information specified for the device will also be deleted. If a deleted device is detected again, the application will provide only the information that has been received since the device was re-added to the table of devices (the date and time of the first detection of the device is also updated).

Device group tree

The device group tree is intended for arranging devices according to their purpose, location, or any other attribute. Devices can be arranged into groups either manually (for example, to designate the location of devices within the facility's industrial structure) or automatically (based on the subnets of device IP addresses, according to the device category, or by vendor).

If a device was not added to any of the groups, this device is assigned to the top level of the group tree hierarchy. By default, devices that are automatically added to the table are not put into groups.

Users with any role except the Operator role can put devices into groups.

You can find out which devices belong to groups when viewing the table of devices. Paths to groups are indicated in the **Group** column. Device groups are also displayed on the network interaction map. However, devices that are in these groups might not be displayed if they do not satisfy the settings for filtering objects on the network interaction map.

Monitoring the network behavior of devices

For each device that is known to the application, you can monitor its network activity by viewing information about the network behavior of this device. The information is displayed in the device details area on the **Network behavior** tab.

Widgets are used to display information about the device's network behavior. Data in widgets is updated in online mode.

The **Network behavior** tab contains the following widgets:

- **Network Interaction Control**. In this widget, the application displays the following information:
  - Current status of monitoring the device's network interactions based on Interaction Control rules (*Enabled* or *Suspended*)
  - Number of Interaction Control rules that specify the device's address information (total number, number of enabled rules, number of disabled rules).
- **Learning quality**. In this widget, the application displays the following information:
  - Current status of compliance of detected device interactions with enabled Interaction Control rules (*OK* or *Anomalies detected*)
  - Number of unprocessed events that were registered due to non-compliance of detected device interactions with enabled Interaction Control rules (total number, number of Network Integrity Control (NIC) events, number of Command Control (CC) events)
- **Network statistics**. In this widget, the application displays the following information:
  - Amount of data received by the device.
  - Amount of data sent by the device.
  - Number of active network sessions.

Some quantitative values in widgets allow you to navigate to the corresponding sections of the application web interface. For example, you can use your mouse to select the displayed number of network sessions to view details about these sessions in the **Network map** section on the **Network sessions** tab.

To clearly display the current status in the **Network Interaction Control** and **Learning quality** widgets, the application uses the appropriate color to highlight the line on the left-side border of the widget. When Interaction Control is configured, green lines on the left-side borders of these two widgets indicate that the application is monitoring the network behavior of the device and all detected interactions comply with the current allow rules for this device.

If the color of the line on the left-side border of the **Network Interaction Control** and/or **Learning quality** widget is not green, you need to check whether this device is functioning correctly and return it to its normal operating mode (if necessary). For example, if a device is involved in preventive maintenance and commissioning operations, the application may register events based on Network Integrity Control or Command Control technology, which results in a switch to the *Anomalies detected* status in the **Learning quality** widget. In this case, you can wait until the end of preventive and commissioning operations and the device will then continue operating normally.

After checking whether the device is functioning correctly, a user with the appropriate permissions can do the following:

- To return the *Enabled* status in the **Network Interaction Control** widget, resume monitoring to track the device's network interactions.
- To return the *OK* status in the **Learning quality** widget, complete the device learning or reset network behavior deviations.

Resetting deviations in the network behavior of devices

When Interaction Control technologies are running in monitoring mode, the application registers events whenever detected interactions between devices do not comply with the enabled Interaction Control rules. Such events are considered *deviations in the network behavior* of devices. If a device was not running in normal operating mode when events were registered (for example, while the device was involved in maintenance and commissioning operations), you can reset the network behavior deviations for this device.

After you reset network behavior deviations, the application assigns the *Resolved* status to all events that are deviations and are related to the selected devices. However, allow rules are not automatically created based on these events.

You can view information about the number of unprocessed events that were registered while monitoring the network interactions of a device. The information is displayed in the device details area on the **Network behavior** tab. To view detailed information about the registered events, you can navigate to the table of events by using the **Learning quality** widget.

To reset deviations in the network behavior of devices:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. Select the **Assets** section.
3. On the **Devices** tab, select the devices for which you want to reset the network behavior deviations.
4. Right-click to open the context menu.
5. In the context menu, select **Reset anomalies**.

   A window with a confirmation prompt opens.
6. If there are risks associated with the network behavior deviation events of the selected devices and you want to assign the *Accepted* status to all of these risks at the same time, select the **Assign the Accepted status for risks related to the events** check box.
7. In the prompt window, confirm that you want to reset the network behavior deviations for the selected devices.

Monitoring read and write of PLC projects

Kaspersky Industrial CyberSecurity for Networks can monitor industrial network traffic for information about PLC projects and compare this information with previously received information about PLC projects.

A PLC project is a microprogram written for a PLC. A PLC project is stored in PLC memory and is run as part of the industrial process that uses the PLC. A PLC project may consist of blocks that are individually transmitted and received over the network when the project is read or written.

Information about a PLC project/block may be received by the application when it detects operations for reading a project/block from a PLC or writing a project/block to a PLC. The obtained information is saved in Kaspersky Industrial CyberSecurity for Networks. The next time it detects a project/block write or read operation, the application compares the received information about the project/block with the saved information. If the received information about a project/block does not match the latest saved information about that project/block (including when there is no saved information), the application registers the corresponding event.

Receiving information about PLC projects is supported for the following classes of devices:

- Emerson DeltaV
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- Siemens SIPROTEC 4 series

You do not need to add Process Control settings for devices to monitor read/write of PLC projects. Read/write of PLC projects is monitored for all detected devices of the listed classes.

For each device, the application saves no more than 100 different variants of PLC projects. If a PLC project is transmitted or received by individual blocks, up to 100 different variants of each block are saved.

If the maximum number of saved PLC projects (or PLC project blocks with the same name) has been reached for a device, the application saves a newly detected project/block in place of the oldest project/block.

When monitoring read/write of PLC projects, the application registers events based on Asset Management technology. Events are registered with system event types that are assigned the following codes:

- Codes of event types when a PLC project/block is read:
  - 4000005200 – for a detected read of an unknown block of a project from a PLC (if there is no saved information about this block).
  - 4000005201 – for a detected read of a known block of a project from a PLC (if there is saved information about this block but the obtained information does not match the latest saved information about this block).
  - 4000005204 – for a detected read of an unknown project from a PLC (if there is no saved information about this project).
  - 4000005205 – for a detected read of a known project from a PLC (if there is saved information about this project but the obtained information does not match the latest saved information about this project).
- Codes of event types when a project/block is written to a PLC:
  - 4000005202 – for a detected write of a new block of a project to a PLC (if there is no saved information about this block).
  - 4000005203 – for a detected write of a known block of a project to a PLC (if there is saved information about this block but the obtained information does not match the latest saved information about this block).

- 4000005206 – for a detected write of a new project to a PLC (if there is no saved information about this project).
- 4000005207 – for a detected write of a known project to a PLC (if there is saved information about this project but the obtained information does not match the latest saved information about this project).

You can configure the available settings for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Monitoring OT devices equipment

Kaspersky Industrial CyberSecurity for Networks can monitor equipment on specialized OT devices, such as PLCs, that automate a process. Equipment monitoring is supported for the following classes of devices:

- Emerson DeltaV
- Rockwell Automation Allen-Bradley ControlLogix series
- Rockwell Automation Allen-Bradley CompactLogix series
- Schneider Electric Modicon M340
- Schneider Electric Modicon M580
- Siemens SIMATIC S7-300
- Siemens SIMATIC S7-400
- Siemens SIMATIC S7-1200
- Siemens SIMATIC S7-1500
- PLC based on the CODESYS V3 platform (for example, Prosoft-Systems Regul R500)

The application receives information about OT device equipment via **Active Poll** connectors. After adding connectors to the application, you can use these to get information when running the following types of security audit jobs:

- Configuration control jobs. We recommend this job type if you want to use **Archive versions** or **Compare to golden configuration** configuration processing for information about equipment connected to OT devices. To obtain equipment information, select the **PLC** device type when adding a configuration control job.
- Active polling jobs. We recommend this job type if you want to receive further information available from the provided active polling methods along with equipment information. To obtain information about OT device equipment, select **Industrial device extended configuration**, and then select the appropriate methods of getting advanced configuration depending on selected devices when adding an active polling job.

After scanning an OT device as part of a configuration control or active polling job, the application updates the equipment information for the device. The information for which automatic update is disabled upon adding a device or changing the device information is not updated. The capability to disable automatic update is not available for some equipment details.

Monitoring OT device equipment helps the application to get information listed in the table below.

Information type	Displayed on the tab in the device details area	Ability to disable automatic update
Graphical layout of modules in slots	**Equipment**	—
Details of each module	**Equipment**, **Configurations**	—
Advanced device information in the form of key entries and key values, such as memory status and device security settings	**Equipment**, **Configurations**	—
Details of the PLC project and project blocks	**Configurations**	—
Hardware vendor	**General**	✓
Hardware model	**General**	✓
Hardware version	**General**	✓
Software version	**General**	✓

In addition to the information listed above, the content of logs stored in the Central Processing Unit (CPU) module can be downloaded to the application. If the device has more than one CPU module connected to it, the logs specific to the module that the Kaspersky Industrial CyberSecurity for Networks connector connected to are downloaded. You can download a file with device logs by using the link on the **Equipment** tab in the device details area.

Monitoring Windows and Linux device equipment

Kaspersky Industrial CyberSecurity for Networks can monitor equipment on devices running Windows and Linux. While monitoring equipment, the application automatically receives information about the device equipment and registers events when the equipment or its characteristics change.

Equipment monitoring on Windows and Linux devices depends on the presence of Endpoint Agent on the devices and an integration between EPP applications and Kaspersky Industrial CyberSecurity for Networks being set up. Therefore, to use the equipment monitoring functionality, prepare the application to receive data from EPP applications. However, asset management methods for device activity detection and device information detection must be enabled on the integration server nodes.

The Windows/Linux equipment information is updated once a day. The information for which automatic update is disabled upon adding a device or changing the device information is not updated. The capability to disable automatic update is not available for some equipment details.

Windows and Linux equipment monitoring helps the application to get the information listed in the table below.

Information obtained by monitoring equipment on Windows and Linux devices

Information type	Displayed on the tab in the device details area	Ability to disable automatic update
Processors	**Equipment**	—
BIOS	**Equipment**	—
RAM	**Equipment**	—
Local drives	**Equipment**	—
Optical drives	**Equipment**	—
USB devices	**Equipment**	—
Network interfaces with MAC address	**Addresses**	✓
Hardware vendor	**General**	✓

Information type	Displayed on the tab in the device details area	Ability to disable automatic update
Hardware model	**General**	✓
Hardware version	**General**	✓

When monitoring equipment on Windows and Linux devices, the application logs events through Asset Management. Events are registered with system event types that are assigned the following codes:

- 4000005015 – for an event of adding, changing, or deleting any of the following types of information:
  - Processors
  - BIOS
  - RAM
  - Local drives
  - Optical drives
  - USB devices
- 4000005008 – for the event of receiving new information about the network interface.
- 4000005004 – for the event of receiving new information about the vendor, model, or hardware version.

You can configure the available settings for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Monitoring device users

Kaspersky Industrial CyberSecurity for Networks can monitor user accounts on devices it knows about. When monitoring users, it automatically receives information about accounts registered in the operating systems of these devices. The application uses these details to create user tables.

After receiving account details, the application uses this information to monitor all user accounts on the devices, with the exception of certain local system accounts that can only be used by operating system services. For example, the application does not control the LocalSystem and NetworkService accounts used on the devices with Windows operating systems.

To use the user monitoring feature, asset management methods for device activity detection and device information detection must be enabled. These methods must be enabled on all nodes where the application components from which information is received are installed.

User monitoring relies on data from the following source types:

1. **OVAL scanning**: software components that scan devices according to built-in OVAL rules, such as EPP applications that send extended device data on demand to Kaspersky Industrial CyberSecurity for Networks or nodes with installed application components that connect to devices remotely when scanning devices as part of a configuration monitoring job.

2. **Telemetry (Endpoint Agent)**: EPP applications that send basic data on devices and running processes (telemetry data) to Kaspersky Industrial CyberSecurity for Networks.

3. **Traffic**: monitoring points where the incoming traffic is analyzed according to the rules for identifying information about devices and the protocols of communication between devices.

4. **External source**: applications that use the Kaspersky Industrial CyberSecurity for Networks API and send user details to Kaspersky Industrial CyberSecurity for Networks.

The sources are listed in the descending order of priority of data coming from them. When processing user details, the application follows data source priority. Users' details from a higher-priority source can overwrite information from other sources. The application also automatically deletes from the tables those user accounts whose details were previously received from the **External source** and **OVAL scanning** sources, but which are not present in the new data received from these sources.

If needed, users with the Administrator of Security Officer role can manually delete user accounts.

You can view information about the users in the **Assets** section of the **Users** tab. When viewing the users table, you can configure, filter, search, and sort records and navigate to the related items.

The all users table is limited to 200,000 items.

The application displays the following device user details in the table and details area for the selected user:

- **User ID**: the user identifier assigned in Kaspersky Industrial CyberSecurity for Networks
- **User name**: the user account name that does not specify the device domain or network name
- **Full name**: the user account name that specifies the device domain name or network name
- **Groups**: the names of user groups of which the user account is a member
- **Device**: device name and address
- **Source**: user data source type
- **SID**: user security identifier
- **Account status**: status that reflects the received parameter value for enabling and disabling the account use
- **Lock**: status that reflects a received account lock parameter value
- **Change password at next logon**: flag that indicates whether the user will be required to reset their password the next time they sign in
- **Block password change by user**: flag that indicates whether the user is prohibited from changing their password
- **Password validity period**: status that reflects a password expiration enabled/disabled value received
- **Data received**: the date and time when account details were last received
- **Description**: the description set for the account

When monitoring users, the application uses the Asset Management technology for event logging. The events are registered using the system event type that is assigned the code 4000005600. Events are logged when user accounts on devices are automatically added, modified, or deleted.

You can configure the available settings for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Monitoring device applications and patches

Kaspersky Industrial CyberSecurity for Networks can monitor applications and patches installed on devices it knows about. When monitoring applications and patches, it automatically receives information about software installed and registered in the operating systems of the devices. The application uses these details to generate application and patch tables.

To use the application and patch monitoring feature, asset management methods for device activity detection and device information detection must be enabled. These methods must be enabled on all nodes where the application components from which information is received are installed.

Application and patch monitoring relies on data from the following source types:

1. **OVAL scanning**: software components that scan devices according to built-in OVAL rules, such as EPP applications that send extended device data on demand to Kaspersky Industrial CyberSecurity for Networks or nodes with installed application components that connect to devices remotely when scanning devices as part of a configuration monitoring job.

2. **External source**: applications that use the Kaspersky Industrial CyberSecurity for Networks API and send application and patch details to Kaspersky Industrial CyberSecurity for Networks.

The sources are listed in the descending order of priority of data coming from them. When processing application and patch details, the application follows data source priority. Application and patch details from a higher-priority source can overwrite information from other sources. The application also automatically deletes from the tables those applications and patches whose details were previously received, but such applications or patches are not present in the new data received from these sources.

You can view applications and patches details in the following tables:

- The all applications table under **Assets** on the **Applications** tab.

  This table displays information about all applications whose data has been received by the application. When viewing the all applications table, you can configure, filter, search, sort, and navigate to related items.

- The all patches table under **Assets** on the **Patches** tab.

  This table displays information about all patches whose data has been received by the application. When viewing the all patches table, you can configure, filter, search, sort, and navigate to related items.

The all applications and all patches tables are limited to 200,000 items each.

The application displays the following device application details in the table and details area for the selected application:

- **Application ID**: the application identifier assigned in Kaspersky Industrial CyberSecurity for Networks
- **Name**: application name
- **Vendor**: application vendor name
- **Device**: device name and address
- **Source**: application data source type

- **Installed**: the date and time when the application was installed
- **Size**: the amount of disk space used by the application files
- **Version**: application version number
- **Data received**: the date and time when application details were last received
- **Description**: the description set for the application

The application displays the following device patch details in the table and details area for the selected patch:

- **Patch ID**: the patch identifier assigned in Kaspersky Industrial CyberSecurity for Networks
- **Name**: patch name
- **Product**: the name of the patched software product
- **Version**: patch version number
- **Vendor**: patch vendor name
- **Device**: device name and address
- **Source**: patch data source type
- **Installed**: the date and time when the patch was installed
- **Data received**: the date and time when patch details were last received
- **Description**: the description set for the patch

When monitoring applications and patches, the application uses the Asset Management technology for event logging. Events are registered with system event types that are assigned the following codes:

- 4000005601: for application added or removed events
- 4000005602: for patch added or removed events

You can configure the available settings for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Launch control of executable files on devices

Kaspersky Industrial CyberSecurity for Networks can control the launch of executable files on the devices known to the application. Monitoring of executable file launches relies on data from EPP applications or applications that use the Kaspersky Industrial CyberSecurity for Networks API. The application uses the received data to create the table of executable files.

Automatic receipt of data about executable file launches is available for devices with Endpoint Agent, which communicates with the EPP application and sends basic data on the devices and running processes (telemetry data) to Kaspersky Industrial CyberSecurity for Networks. The application specifies the **Telemetry (Endpoint Agent)** source for this data. If the data about an executable file run is received only from the application that uses the Kaspersky Industrial CyberSecurity for Networks API, the application sets the data source value to **External source** for this file.

To receive data about executable file runs from the **Telemetry (Endpoint Agent)** source, asset management methods must be enabled for detecting device activity and device information. These methods must be enabled on all nodes where the application components from which EPP applications information is received are installed.

The table of executable files has the following limitations on the number and storage time of elements:

- The total number of executable files can be no more than 100 thousand.

  If the maximum number of executable files is reached, the application automatically deletes 10% of the oldest records.

- The maximum storage time for an executable file until the next execution data for this file is received can be no more than 90 days.

  If no new data about the run of the executable file was received before the maximum storage time expires, the application automatically deletes the entry about this file.

If needed, users with the Administrator or Security Officer role can manually delete executable files.

You can view information about executable files on the **Executable files** tab in the **Assets** section. When viewing the executable files table, you can configure, filter, search, sort, and navigate to related items.

The application displays the following device executable files details in the table and details area for the selected file:

- **File ID** is the file identifier assigned in Kaspersky Industrial CyberSecurity for Networks.
- **Device** is a device name and address.
- **Name** is the application name and version, or file name.
- **Data received** is the date and time when file details were last received.
- **Product** is the name of the software product saved in the device operating system.
- **Product version** is the version of the software product saved in the device operating system.
- **Vendor** is the application vendor name.
- **Path** is the full path to the file.
- **File size** is the amount of disk space used by the file.
- **MD5 hash** is the file checksum obtained using the MD5 hash algorithm.
- **SHA256 hash** is the file checksum obtained using the SHA256 hash algorithm.
- **Signature** is the result of the file digital signature verification. It's either **Valid** (if the digital signature was verified successfully) or **Invalid** (for example, if the certificate has expired).

- **Created** is the date and time when the file was created.
- **Changed** is the date and time when the file was last modified.
- **Source** is the file data source type.
- **Attributes** is the list of file attributes.
- **Description** is the description set for the file.

Device configuration control

Kaspersky Industrial CyberSecurity for Networks provides the capabilities for viewing information about device configurations obtained as a result of configuration control jobs. You can view information about the configurations of the selected device in the device details area on the **Configurations** tab.

The application displays the following information about the received configurations of the selected device in the table on the **Configurations** tab:

- **Configuration type** – the name of the received configuration type (such as **Users**, where the information about the device users is stored).
- **Last configuration received** – the date and time when the configuration type was last received if display of the last received configurations is enabled.
- **Golden configuration received** – the date and time when the golden configuration was received if display of the golden configurations is enabled.
- **Total configurations** – the total number of the type configurations obtained during configuration control jobs. The count includes potential duplicate configuration data, which may only vary by timestamp.

Golden configuration types are marked with a crown icon.

When you select a configuration type, you will see a window containing detailed information about this type.

For convenient viewing of the device configuration information, you can compare saved configurations using Kaspersky Industrial CyberSecurity for Networks.

When controlling device configurations, the application uses the Asset Management technology for event logging. Events are registered with system event types that are assigned the following codes:

- 4000005603 – events of detecting changes when comparing with the previous configuration based on the results of device scans (for the jobs run in the **Update only** and/or **Archive versions** configuration processing modes).
- 4000005604 – events of detecting changes when comparing with the golden configuration based on the results of device scans (for the jobs run in the **Compare to golden configuration** processing mode).

You can configure the available settings for event types under **Settings** → **Event types**.

You can view information about registered events when connected to the Server through the web interface.

Comparison of saved device configurations

Based on the device scan results as part of configuration control jobs, the application can save the received configurations for each device. You can compare the saved device configurations when working with the table of devices.

Unlike change detection and event enrollment algorithms for device configuration control, when using the function for comparing saved configurations, you can compare any saved device configurations (not just the last received configuration with the previous or golden configuration). This option is available if the device has stored configurations that were captured as a result of running jobs.

When comparing configurations for a device, bear in mind that configurations received by the application are retained for a limited time and automatically deleted as new ones come in. Deletion frequency depends on how much data comes in and how frequently. Only the golden and the last received configurations are not automatically deleted. If needed, users with any role except the Operator role can set any saved configurations as golden configurations.

To compare saved device configurations:

1. On the **Devices** tab in the **Assets** section, select the relevant device.

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

2. On the **Configurations** tab, in the details area, select the table row with the desired configuration type, such as **Users**, which stores user data. The selected type must have a value of at least 2 in the **Total configurations** column.

   You will see a window containing detailed information about the selected configuration type.

3. Click **Compare**.

   You will see a window containing the results of comparing the selected configuration type with the previous or the golden configuration. The date and time when the compared configurations were received are displayed in the upper part of the window.

4. Perform the following actions:

   - To compare with another saved configuration, select the date and time when the desired configuration was received from the drop-down list.
   - If required, change the position of the compared configurations relative to each other. To do so, use the button between the drop-down lists with dates and times.
   - If necessary, disable the display of unmodified blocks in the compared configurations.

Working with the network interaction map

The network interaction map is a visual representation of detected communications between the devices in the industrial network. You can use the network interaction map to view information about communication between devices during various time periods.

The following objects can be displayed on the network interaction map:

- Nodes. These objects designate the sources and destinations of network packets.
- Device groups. These objects correspond to groups in the device group tree. Groups contain nodes that represent the devices and child groups embedded in those groups.
- Links. These objects represent connections between nodes.

Nodes and links appear on the network interaction map based on data received from traffic or from EPP applications for a specific time interval. Device groups are continually displayed.

If necessary, you can filter nodes and links. By default, the network interaction map displays objects in real time with a defined filtering period of one hour.

Objects with issues are visually distinguished on the network interaction map. The application considers the following to be objects with issues:

- A node, if there are unprocessed events with a score 4.0 or higher associated with this node, or if this node represents a device with a status of *Unauthorized*.
- A connection, if there are events with a score 4.0 or higher associated with this connection. Events registered during the defined object filtering period are taken into account. However, the current status of events is not taken into account.
- Group that contains devices with issues, or whose nodes have links with issues. This includes objects within the group and within any child group of all nesting levels.

Nodes on the network interaction map

Nodes on the network interaction map can be of the following types:

- A device that is known to the application. This type of node represents a device that is listed in the table of devices.
- 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 table of devices. Such a node may appear on the network interaction map, for example, if network packets are sent using the `ping` command to the address of a non-existent device. Nodes corresponding to unknown devices are displayed individually if their total number does not exceed 100 (according to the current filter settings on the network interaction map). If the number of nodes exceeds this limit, one consolidated node of unknown devices is displayed.
- WAN. This type of node represents devices of a Wide Area Network with which industrial network devices connect. WAN devices are any devices whose IP addresses belong only to **Public** subnets known to the application.

Displayed information on nodes representing devices

The following information is displayed for the nodes corresponding to known devices when the network interaction map is maximized:

- Assigned device name.
- Device category icon.
- IP address of the device (If an IP address is not assigned, the MAC address is displayed).
- Various icons depending on fulfillment of the following conditions:
  - If the router indicator has been set for the device.
  - If an EPP application is installed on the device (the color of the icon depends on the connection status).
  - If the device has a status of *Archived*.
- The thick line on the left border of a node has one of the following colors depending on the device's security state:
  - Green signifies the *OK* security state.
  - Yellow signifies the *Warning* security state.
  - Red signifies the *Critical* security state.

If a device has a status of *Unauthorized* or has a security state different from *OK*, the node has a red background.

Information displayed on nodes representing unknown devices

The following information is displayed for the nodes corresponding to unknown devices when the network interaction map is maximized:

- If a node represents one unknown device, the IP address or MAC address of the device is displayed. For a consolidated node of unknown devices (a node that combines more than 100 unknown devices), **Unknown devices** is displayed.
- Icon for an unknown device and its status .

Nodes representing devices that are unknown to the application have a gray background.

Displayed information on WAN nodes

The following information is displayed for WAN nodes when the network interaction map is maximized:

- Node name: **WAN**.
- WAN node icon.

Groups of devices on the network interaction map

Groups belonging to the device group tree may be collapsed or expanded on the network interaction map. Collapsed groups are displayed as icons similar to nodes. Expanded groups are displayed as windows containing their embedded nodes and other groups.

Displayed information on collapsed groups

If a group is collapsed, the following information is displayed when the network interaction map is maximized:

- Group name.
- Number of devices that satisfy the current filter settings on the network interaction map. This number includes devices within the group and within its child groups in all nesting levels.
- Number of child groups in all nesting levels.

If a group contains devices or links with issues (including in child groups of any nesting level), the border of this group is colored red.

Displayed information on expanded groups

The window of an expanded group contains a title with the group name and an area for displaying objects. The group window displays the devices included in this group, and the child groups of the next nesting level. Of the devices included in the group, only the devices that meet the current filter settings are displayed on the network interaction map.

If a group contains devices or links with issues (including in child groups of any nesting level), the window has a red background.

Collapsing and expanding groups

If a group is collapsed, you can expand it by double-clicking the icon of the group. If a group is expanded, you can collapse it by double-clicking the header of this group's window or by clicking the button in the header.

To simultaneously expand multiple collapsed groups:

1. On the network interaction map, select multiple collapsed groups by performing one of the following actions:
   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant groups.
   - Hold down the **CTRL** key and use your mouse to select the relevant collapsed groups.
2. Click in the toolbar located in the left part of the network interaction map display area (the button is available if at least one collapsed group is selected).

To simultaneously collapse all expanded groups:

Click in the toolbar located in the left part of the network interaction map display area (the button is available if at least one group is expanded).

Links on the network interaction map

Links on the network interaction map are identified based on detected network packets for which the source and destination addresses can be mapped to the addresses of nodes.

Each link shows two sides of communication. A communication side in a link may be one of the following objects on the network interaction map:

- One of the following types of nodes:
  - A device that is known to the application.
  - A device that is unknown to the application.
  - Consolidated node of unknown devices – if the link shows communication with one or more unknown devices of this node.
  - WAN node – if the link shows communication in which the source of network packets is a WAN device (the IP address belongs only to **Public** networks known to the application).
- Collapsed group, if the link shows communication with one or more devices in this group.

Depending on the scores of the events registered when communications are detected, the link may have the one of following colors:

- Gray – the communication did not cause event registration, or only events with score of 0.0–3.9 were registered.
- Red – the communication caused the registration of events with score of 4.0–10.0.

Events registered during the defined object filtering period are taken into account for links. However, the current status of events is not taken into account.

The application saves connection data in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for the network interaction map when configuring data storage settings on the Server node.

Viewing details about objects

Detailed information about objects on the network interaction map are displayed in the details area. To display detailed information, you can use your mouse to select an object (if you want to view information about a group, you must first collapse the group).

The following information is displayed for nodes:

- If a node represents a known device, the details area displays the same information that is displayed in the table of devices.
- If a node represents one unknown device, the details area displays the MAC address and/or IP address of the device (including the names of address spaces if additional address spaces were added to the application).
- If a consolidated node of unknown devices is selected, the following information is displayed:
  - Number of nodes combined by this node under the current filter settings.
  - **IP addresses** – number of IP addresses of unknown devices and the first 100 IP addresses (including the names of address spaces if additional address spaces were added to the application). This section is displayed if there are nodes with IP addresses among the nodes of unknown devices.
  - **MAC addresses** – number of MAC addresses of unknown devices and the first 100 MAC addresses (including the names of address spaces if additional address spaces were added to the application). This section is displayed if there are nodes with MAC addresses among the nodes of unknown devices.

The following information is displayed for groups:

- **Parent group** – path to the group in the device group tree. If a group belongs to the top hierarchy level, **N/A (this is a top-level group)** is displayed.
- Number of devices and groups within the selected group and its child groups of all nesting levels.
- Information about the number of objects with issues within the selected group and its child groups of all nesting levels. If there are no such objects, the *OK* security state is displayed.

The following information is displayed for links:

- **Severity** – icon corresponding to the maximum severity level of events associated with the link. If no event is associated with the link, **No events** is displayed. Events registered during the defined object filtering period are taken into account. However, the current status of events is not taken into account.
- Sections containing basic information about the first and second sides of communication:
  - If the side of communication is a node of a known device or a node of an unknown device, the section displays the name or address of the device/device, category, and address information (for a known device, address information is provided only for those network interfaces that were used during the communication). The device status is also displayed for known devices.
  - If the side of communication is a collapsed group, the section displays the name of the group and the number of devices and child groups within it.
  - If the side of communication is a consolidated node of unknown devices, the section displays the **Unknown devices** node name and the number of nodes combined within that node.
- **Protocols** – section containing a list of protocols used for communication. The volume of transmitted data calculated for detected network packets is specified for each protocol. This section is not displayed if one of the sides of communication is a consolidated node of unknown devices.

Changing the scale of the network interaction map

The network interaction map can be displayed in a scale of 1–100%. The current scale is displayed in the toolbar located in the left part of the network interaction map display area.

To change the scale of the network interaction 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 interaction map reduces the amount of information that is displayed for the nodes and collapsed groups.

If the display scale is less than 25%, icons and text information are not displayed in nodes and collapsed groups. The appearance of nodes and collapsed groups may change as follows:

- On a node representing a device that is known to the application (device), the upper-right corner displays the device status as a triangle in one of the following colors:
  - Green signifies that the device has a status of *Authorized*.
  - Red signifies that the device has a status of *Unauthorized*.
  - Gray signifies that the device has a status of *Archived*.
- A thick black line on the left border of the node appears on the WAN node.

- On a collapsed group, the upper-right corner displays a triangle indicating the presence of objects with issues. The triangle has one of the following colors:
  - Green means that the group does not contain objects with issues.
  - Red means that the group contains objects with issues.

Positioning the network interaction map

If necessary, you can change the positioning of the network interaction map manually or automatically. Automatic positioning lets you move the network interaction map and change its scale to display all nodes that satisfy the defined filter settings, as well as all expanded groups.

To manually position the network interaction map:

1. Position the mouse pointer over any part of the network interaction map that is not occupied by objects.
2. Click and hold the left mouse button to drag the network interaction map.

To automatically position the network interaction map:

Click the button in the toolbar located in the left part of the network interaction map display area.

The positioning and the scale of the network interaction map will change to display all nodes and expanded groups.

Pinning and unpinning nodes and groups

By default, nodes and collapsed groups are not pinned on the network interaction map. Unpinned nodes and collapsed groups may be automatically arranged for optimal display of other objects.

Nodes and groups are pinned when their location is changed manually or when automatically arranged. You can also pin the current location of displayed objects without moving them.

To pin and unpin objects without moving them, you can use the following interface elements:

- The buttons in the toolbar located in the left part of the network interaction map display area. You can use the and buttons to pin and unpin all nodes and groups displayed on the network interaction map (including nodes in expanded groups).
- Buttons in the expanded group's window header. You can use the and buttons to pin and unpin only nodes and groups in the window of the expanded group (but not in windows of nested groups).

The buttons are available if the network interaction map contains the objects to which the corresponding actions can be applied.

After the location of a node or collapsed group is pinned, the icon appears in the upper-right corner of this element (if the scale of the network interaction map is not less than 25%). You can also use this icon to unpin the object.

The location of a pinned node or pinned group is retained. If a pinned node disappears from the network interaction map (for example, as a result of filtering), this node will be displayed in the same location the next time it appears.

Manually changing the location of nodes and groups

You can manually change location of nodes and groups on the network interaction map by arranging them in the most convenient way for you.

After their arrangement, nodes and groups are locked (pinned) in their new location. If necessary, you can unpin these objects.

Objects that are included in groups can be moved only within the windows of these groups.

To change the location of nodes and/or collapsed groups:

1. On the network interaction map, select one or multiple objects corresponding to nodes and/or collapsed groups.

   To select multiple nodes and/or collapsed groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

2. Use your mouse to drag the selected objects to the necessary location.

After they are moved, nodes and collapsed groups will remain pinned. The icon appears in these objects.

To change the location of an expanded group:

Move the cursor over the expanded group's window title, left-click and drag the window to the necessary location.

Automatic arrangement of nodes and groups

For optimal arrangement of objects on the network interaction map, you can use algorithms to automatically change the location (arrangement) of nodes and groups. The following algorithms are provided:

- Radial arrangement.
- Grid-aligned arrangement.

You can use automatic arrangement algorithms for the following objects:

- All displayed nodes and groups at the top level of the hierarchy within the group tree. Automatic arrangement is performed using the (radial arrangement) button and the (grid-aligned arrangement) button in the toolbar located in the left part of the network interaction map display area.

- All displayed nodes and groups within the expanded group. Automatic arrangement is performed by using the (radial arrangement) button and (grid-aligned arrangement) button in the expanded group's window header.

- Only selected nodes and collapsed groups. Before performing automatic arrangement, you need to select at least three nodes and/or collapsed groups within the expanded group or at the top level of the hierarchy. To select multiple objects, you can use the mouse to select a rectangular area containing the relevant objects while holding down the **SHIFT** key, or select the relevant objects with the mouse while holding down the **CTRL** key. Automatic arrangement is performed using the (radial arrangement) button and the (grid-aligned arrangement) button in the toolbar located in the left part of the network interaction map display area.

After automatic arrangement, nodes and groups are locked (pinned) in their new location. The icon appears in these objects. If necessary, you can unpin these objects.

Searching for nodes on the network map

You can search nodes on the network interaction map based on information about these nodes. This search involves all nodes that meet the current filter settings, including those located in collapsed groups or outside of the displayed part of the network interaction map.

For nodes representing known devices, the search is performed in all columns of the table of devices except **Status**, **Security state**, **Last seen**, **Last modified**, and **Created**. The search is also performed in the values of custom fields for devices.

To find the nodes on the network interaction map:

In the **Network map** section, enter your search query into the **Search nodes** field. The search is initiated as you type characters in the search field.

If nodes that satisfy the search query are found, the contours of these nodes are highlighted in yellow. The contours of collapsed groups in which nodes were found are highlighted in the same way. Meanwhile, the right part of the **Search nodes** field will display the following items:

- Sequence number of the currently selected object (node or collapsed group containing the found nodes) among the search results.

- Total number of found objects (nodes and/or collapsed groups containing the found nodes).

  The number of nodes in collapsed groups is not taken into account in the total number of found objects. If you want the nodes in groups to also be taken into account in the search results, expand the collapsed groups.

- Arrows for moving between found objects. Arrow movements proceed in alphabetical order of the names of found objects. When moving to the next object, the network interaction map is automatically positioned to display this object.

Filtering objects on the network interaction map

This section provides instructions on filtering objects on the network interaction map to limit the number of nodes and links displayed.

Comprehensive filtering of nodes and links

This section contains instructions on comprehensive filtering of nodes and links.

Filtering using a period on the time scale

To filter nodes and links, you can choose the relevant period of time on the time scale. The time scale is displayed in the lower part of the **Network interaction map** tab of the **Network map** section.

The time scale contains the following items:

- Time scale start date and time.
- Periods when events with scores of 4.0 and above were registered. These periods are displayed as red strips in the lower part of the time scale. The periods are not displayed if a duration of more than seven days is defined for the time scale.
- Filtering period. This period is displayed as a yellow band lined with buttons for moving the boundaries.
- Chart of the volume of traffic processed by the application. The chart is not displayed if a duration of more than seven days is defined for the time scale.
- End of the time scale. Depending on the arrangement of the filtering period, the end of the time scale is displayed as a date and time (if the date and time are defined) or as a **Now** link.

The following types of filtering periods are provided:

- Period correlated to the current moment. The right-side boundary of this period corresponds to the time scale boundary designating the current moment in time.
- Period not correlated to the current moment. This type of period may be arranged in any part of the time scale.

To configure object filtering by a period correlated to the current moment:

1. Click **Now** on the right of the time scale. This button is not displayed if the period is already correlated to the current moment.

2. If it is necessary to specify a different period duration, perform one of the following actions:

   - Move the left border of the yellow band of the period to the necessary position (the maximum duration of the period is 7 days).

   - Open the configuration window by clicking the button above the yellow band of the period, select the **Anchor to boundary** check box, select the necessary duration (**Hour**, **Day**, or **7 days**), and click **OK**.

The network interaction map shows only the nodes and links for which communications were detected since the beginning of the specified period up to the current moment.

To configure filtering by a period not correlated to the current moment:

1. If the necessary period is not within the time scale, change the values of the date and time for the start and/or end of the time scale:

   a. To change the data and time of the start of the time scale, open the window by clicking the link in the left part of the time scale and select one of the following options:

      - **Day**.

      - **7 days**.

      - **30 days**.

      - **Specify a date**. For this option, specify a date and time in the opened field.

   b. To change the date and time of the end of the time scale, open the window by clicking the link in the right part of the time scale and select one of the following options:

      - **Now**.

      - **Specify a date**. For this option, specify a date and time in the opened field.

2. Specify the necessary period. To do so, do one of the following:

   - Use the mouse to move the period to the relevant place on the time scale.

   - Move one or both of the borders of the yellow band of the period to the necessary part of the time scale (the maximum duration of the period is 7 days).

   - Open the configuration window by clicking the button above the yellow band of the period, select the necessary duration (**Hour**, **Day**, or **7 days**) and click **OK**.

3. If a period is automatically anchored to the current moment (when you move the period to the right-most position, the **Now** button on the right of the time scale is no longer displayed), disable automatic anchoring of the period to the time scale boundary. To do so, open the configuration window by clicking the button above the yellow band of the period, clear the **Anchor to boundary** check box, and click **OK**.

Filtering by registered events

You can configure the network interaction map to show the nodes and links whose information is saved in the events associated with the selected nodes.

The capability to filter by events is available if no more than 200 nodes are selected on the network interaction map. You can select the relevant nodes individually or as part of collapsed groups that include the relevant devices. When a collapsed group is selected, all devices in the child groups of any nesting level are also included in the device selection.

You can use the following methods to filter by event:

- Initial filtering by event. This method is applied if you need to filter objects based on events associated only with the selected nodes.
- Additional filtering by event. This method is applied if initial filtering by events is already performed (for example, when switching to the network interaction map from the table of events) and you need also to filter events associated with additionally selected nodes from the list of nodes displayed on the network interaction map.

To display nodes and links using initial filtering by event:

1. On the network interaction map, select one or multiple objects corresponding to nodes and/or collapsed groups.

   To select multiple nodes and/or groups, do one of the following:

   - Hold down the **SHIFT** key and use your mouse to select a rectangular area containing the relevant objects.
   - Hold down the **CTRL** key and use your mouse to select the relevant objects.

2. In the toolbar above the network interaction map, open the **Event filter** drop-down list.
3. In the drop-down list, select **Filter**.

   The network interaction map displays only the nodes and links whose information is contained in the events associated with the selected nodes. The toolbar located above the network interaction map displays a list containing the IDs of events (IDs are listed in the order in which their associated events were detected).

To add nodes and links to the displayed objects by using additional filtering by event:

1. Make sure that initial filtering by event has been performed. To do so, check for the availability of a list containing event IDs in the toolbar located above the network interaction map.
2. Among the nodes displayed on the network interaction map, select the nodes for which you want to add associated events to the filter.

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

3. In the toolbar above the network interaction map, open the **Event filter** drop-down list.
4. In the drop-down list, select **Add to filter**.

   The network interaction map also displays the nodes and links whose information is contained in the events associated with the selected nodes. The IDs of detected events are added to the list containing IDs in the toolbar.

Filtering of nodes

This section provides instructions on filtering nodes.

Filtering nodes by device status

To filter nodes by device status:

1. In the toolbar above the network interaction map, open the **Device statuses** drop-down list.

   You will see a list containing the names of statuses for known devices (*Unauthorized*, *Authorized*, and *Archived*) and the *Unknown device* status for devices that are unknown to the application.

2. In the drop-down list, select the check boxes for the statuses of devices that need to be displayed on the network interaction map.

3. Click **OK**.

The network interaction map displays only the nodes corresponding to devices with the selected statuses.

Filtering nodes by device security state

To filter nodes by device security state:

1. In the toolbar above the network interaction map, open the **Device states** drop-down list.

   You will see a list containing the names of security states for devices (*OK*, *Warning*, and *Critical*).

2. In the drop-down list, select the check boxes for the security states of nodes that need to be displayed on the network interaction map.

3. Click **OK**.

The network interaction map displays only the nodes corresponding to devices with the selected security states.

Filtering nodes by device category

To filter nodes by device category:

1. In the toolbar above the network interaction map, open the **Device categories** drop-down list.

   You will see a list containing the names of categories for known devices, as well as individual categories for unknown devices and WAN nodes.

2. In the drop-down list, select the check boxes for the categories of devices that need to be displayed on the network interaction map.

3. Click **OK**.

The network interaction map displays only the nodes corresponding to devices with the selected categories.

Enabling and disabling the display of nodes associated with filtered nodes

After filtering nodes, the network interaction map displays only the nodes that satisfy the defined filter settings. In addition, for a node to be displayed on the network interaction map, it must have a connection (link) with another displayed node. If, according to the specified filtering parameters, the network interaction map does not display any node with which a node has interacted, this node is also not displayed on the network interaction 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 interaction map to display all nodes associated with filtered nodes. Together with the nodes that satisfy the defined node filtering criteria, the network interaction map also displays all nodes with which these nodes have interactions (irrespective of the defined filter settings).

For example, if the nodes are filtered by the **PLC** category and you enabled the display of linked nodes, the network interaction map will display all nodes that have communicated with **PLC** category devices. If the display of linked nodes is disabled, the network interaction map will display nodes corresponding only to those **PLC** category devices that have communicated with each other.

To enable or disable the display of nodes associated with filtered nodes:

Use the **Linked devices** toggle switch in the toolbar located above the network interaction map.

Filtering links

This section provides instructions on filtering links.

Filtering links by criticality score

To filter links on the network interaction map by criticality score:

1. In the toolbar above the network interaction map, open the **Scores of links** drop-down list.

   A list is displayed that contains the names of event severity levels with their score ranges (Low (0.0–3.9), Medium (4.0–7.9), High (8.0–10.0)), as well as the **No events** element, which allows you to filter the connections for which no events are registered.

2. In the drop-down list, select the check boxes for those severity levels by which you want to filter links.

3. Click **OK**.

The network interaction map displays only the links associated with events that have the selected severity levels.

Filtering links by communication protocol

To filter links on the network interaction map by communication protocol:

1. In the toolbar above the network interaction 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 interaction map displays only the links for which the selected protocols are used.

Filtering links by OSI model layer

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 interaction map based on the layers of the OSI network model:

1. In the toolbar above the network interaction map, open the **OSI model layers** drop-down list.

   You will see a list containing the names of OSI model layers:

   - **Data Link**. This layer includes the communication links in which MAC addresses were used to communicate with devices.
   - **Network**. This layer includes links in which IP addresses were used to communicate with devices.
2. In the drop-down list, select the check boxes for the OSI model layers whose links need to be displayed on the network interaction map.
3. Click **OK**.

The interaction network map displays only the links that are associated with the selected OSI model layer.

Resetting the filter settings

You can reset the defined settings for filtering nodes and links to their default state.

To reset the defined filter settings on the network interaction map:

In the toolbar above the network interaction map, click **Default filter** (this button is displayed if filter settings are defined).

The network interaction map will display all nodes and links for which communications within the specified period were detected.

Saving and loading network interaction map display settings

This section describes the network interaction map display customization features.

The application lets you save the current network interaction map display settings. A set of saved display settings is called a *view*. You can use views to apply the saved display settings of the network interaction map (for example, to quickly restore the display settings after making some changes, or to work with the network interaction map on a different computer).

When a network interaction map view is saved, the following display settings are saved:

- Scale
- network interaction map positioning
- Location of pinned nodes and groups
- Filtering of nodes and links

The application can save and use no more than 10 groups of settings for the different network interaction map views.

All users can manage the list of network interaction map views (including saving the current display settings).

Adding a new view while saving the current network interaction map display settings

To add a new view while saving the current network interaction map display settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network interaction map** tab in the **Network map** section, configure the display settings of the network interaction map.
3. Open the **Configure network map views** window by clicking **Manage views**.
4. Click **Add**.
5. Type the view name in the entry field.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

A view name must meet the following requirements:

- Must begin and end with any permitted character except a space.
- Must contain 100 characters or less.
- Must not match the name of a different view (not case-sensitive).

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

Updating a view while saving the current network interaction map display settings

To update a view while saving the current network interaction map display settings:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network interaction map** tab in the **Network map** section, configure the display settings of the network interaction map.
3. Open the **Configure network map views** window by clicking **Manage views**.
4. Select the view in which you want to save the current network interaction map display settings.
5. Click **Overwrite**.

   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 interaction map view

To rename a network interaction map view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network interaction map** tab in the **Network map** section, open the **Configure network map views** window by clicking **Manage views**.
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 interaction map view

To delete a network interaction map view:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network interaction map** tab in the **Network map** section, open the **Configure network map views** window by clicking **Manage views**.
3. Select the view that you want to delete.
4. Click **Delete**.

   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 interaction map

To apply saved view settings on the network interaction map:

1. On the **Network interaction map** tab in the **Network map** section, open the **Configure network map views** window by clicking **Manage views**.
2. Select the relevant view in the list.
3. Click **Apply**.

   A window with a confirmation prompt opens.
4. In the prompt window, confirm application of the view.

Downloading traffic when working with the network interaction map

When working with the network interaction map, you can download traffic received by the application via the monitoring points. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads traffic from the traffic dump file storages. Both the internal storage of each node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.

To download traffic when working with the network interaction map:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network interaction map** tab in the **Network map** section, click **Download traffic**.

   The details area appears in the right part of the web interface window.
3. Perform the following actions:

   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

     By default, the period is set to the period configured for filtering specified on the time scale.
   - Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

     If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.
   - If necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points that received the desired traffic.

     By default, all monitoring points available on nodes with the installed application components are specified.
   - If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets belong (this section is displayed if additional address spaces are added to the application).

     By default, all address spaces created in the application are specified.
   - If necessary, enable filtering in the **Filtering using BPF** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets.

     Filtering expression example

     ```
     tcp port 102 or tcp port 502
     ```
   - If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets.

     Filtering expression example

     ```
     ^test.+xABxCD
     ```
4. Click **Download**.

5. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the button in the menu of the application web interface.

      The list of background operations appears.

   b. Wait for the file generation operation to complete.

   c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Network session monitoring

Kaspersky Industrial CyberSecurity for Networks can detect network sessions created by the devices for connecting with other devices in the industrial network traffic. When network sessions are detected, the application registers them and saves information about them. Unlike connections on the network interaction map, registered network sessions provide more detailed information about the device interactions, including because of separate registration of sessions for different ports and protocols that were used in the interactions.

Network session detection can be performed when analyzing traffic received by monitoring points, as well as when receiving data from EPP applications. Each registered network session contains information about the connection between two devices that are interaction sides. A network session is characterized by the address information of the interaction sides (MAC and / or IP addresses), port numbers, and the application protocol that was used for the connection. The first device in a network session is usually the device that initiates the sending of network packets to the other device.

The saved information about network sessions enables an analysis of the network activity of devices, including through the use of Network Anomaly Detection rules. Network Anomaly Detection rule-based analysis utilizes the saved protocol attributes in network sessions (the application supports retention of attributes for the DCE/RPC, DNS, Kerberos, and LDAP protocols). You can also download data on transmitted network packets from traffic dump files.

The application registers network sessions and saves information for analyzing the network activity of devices if the following methods are enabled:

- Network session detection using Asset Management technology.
- Getting attributes of protocols using Process Control technology.

A network session is considered completed if no network packets are sent during one minute within this session or if the network session detection technology is disabled on the corresponding node or monitoring point.

If an excessive number of network sessions are detected, the application applies the following session registration restrictions:

- The number of registered sessions between the two interaction sides using the same application protocol doesn't exceed 1000 per minute
- The total number of registered sessions between the two interaction sides is no more than 5000 per minute

The application saves network session data in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for the network sessions when configuring data storage settings on the Server node in the **Network sessions** section.

You can view information about network sessions on the **Network sessions** tab in the **Network map** section.

Network sessions table

The network sessions table is displayed on the **Network sessions** tab in the **Network map** section.

The network sessions table contains the following information:

- **ID** is the network session identifier assigned in Kaspersky Industrial CyberSecurity for Networks.
- **Status** – the network session status. A registered network session can have one of the following statuses:
  - **Active**. This status is assigned when a network session is registered and is retained as long as devices within this session send network packets.
  - **Closed**. This status is assigned to a network session if no network packets are sent during one minute within this session or if the network session detection technology is disabled on the corresponding node or monitoring point.
- **Side 1** – MAC and/or IP addresses of the first network interaction side. MAC and IP addresses can be enabled and disabled.
- **Side 1 port** – port number of the first side of the interaction.
- **Side 2** – MAC and/or IP addresses of the second network interaction side. MAC and IP addresses can be enabled and disabled.
- **Side 2 port** – port number of the second side of the interaction.
- **Device 1** – name of a device known to the application to which the address information of the first interaction side corresponds.
- **Device 2** – name of a device known to the application to which the address information of the second interaction side corresponds.
- **Transfer protocol** – transport protocol used in the network session.
- **Application protocol** – application layer protocol used in the network session.
- **Current speed** – current data transfer rate in the network session.
- **Average speed** – average data transfer rate in the network session.
- **Total transmitted** – the number of bytes transmitted in the network session.
- **Monitoring points** – names of the monitoring points that receive the network session traffic.
- **Start** – date and time of the first network packet in the network session or the start date and time of the time interval which data is received from the EPP application.

- **Last interaction** – date and time of the last network packet in the network session or the expiration date and time of the time interval which data is received from the EPP application (if only one packet is received in the network session, the value is the same as the **Start** value).

- **Number of packets** – the number of network packets transmitted in the network session.

When viewing the network session table, you can use configuration, filter, search, and sort functions, navigate to the related items, and export data.

When exporting network sessions to JSON format, the file also contains lists of extracted protocol attributes (which the application can analyze using SQL queries in Network Anomaly Detection rules).

Viewing network session details

Detailed information about a network session includes information from the network sessions table and the following fields (if values are available for these fields):

- **Application** on the **Settings** tab: the name of the application that was running when the network session was initiated.

- Text field containing protocol attributes on the **Attributes** tab: a list of received protocol attributes in a network session (which the application can analyze using SQL queries in Network Anomaly Detection rules).

To view information about a network session:

On the **Network sessions** tab in the **Network map** section, select the required network session.

The details area appears in the right part of the web interface window. The details area displays all received information about the network session.

Downloading network session traffic

When viewing the network sessions table, you can download the traffic related to the selected network sessions. The traffic is downloaded to a PCAP file. You can configure network packet filtering to download the relevant data.

The application downloads the network session traffic from the traffic dump file storages. Both the internal storage of a node (created automatically when an application component is installed on the node) and the external storage, if connected on the node, can be used to download traffic.

When downloading the network session traffic, take the following considerations into account:

- Traffic download is possible only for the network sessions registered during the analysis of traffic received at the monitoring points. If a network session was registered based on the data received from the EPP application, the application cannot download the traffic of this session.

- Traffic dump files are temporarily stored in the storages and are automatically deleted as new traffic is received. The frequency of file deletion depends on the amount of traffic received and on the specified application data storage settings. The network session traffic cannot be downloaded if the corresponding traffic dump files are deleted from the repositories.

To download network session traffic:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.
2. On the **Network sessions** tab in the **Network map** section, select the network sessions for which you want to download traffic.

   You can select no more than 100 network sessions.
3. Click **Download traffic**.

   The details area appears in the right part of the web interface window.
4. Perform the following actions:

   - To download traffic for a certain period of time, define the desired boundaries using the **Period of traffic to download** setting.

     By default, the maximum possible period is specified, from the start date and time of the earliest network session to the end date and time of the latest session from the selected sessions. If necessary, you can set boundaries within this period or set an empty value for one of the boundaries (for example, for the right boundary to download new traffic of the sessions that are not yet completed).
   - Set a limit on the maximum volume used for the downloaded traffic in the **Download volume limit** section.

     If the volume of the downloaded traffic exceeds the specified limit, the traffic that arrives later is skipped.
   - If necessary, enable filtering in the **Filtering by monitoring points** section and specify the monitoring points that received the desired traffic.

     By default, the monitoring points that receive the traffic of the selected network sessions are specified.
   - If necessary, enable filtering in the **Filtering by address spaces** section and specify the address spaces to which the addresses in the network packets of the selected network sessions belong (this section is displayed if additional address spaces are added to the application).

     By default, all address spaces created in the application are specified.
   - If necessary, enable filtering in the **Filtering using BPF** section and enter a filtering expression using the Berkeley Packet Filter (BPF) technology based on the address settings of the network packets of the selected network session.

     ```
     Filtering expression example
     ```

     ```
     tcp port 102 or tcp port 502
     ```
   - If necessary, enable filtering in the **Filtering using regular expressions** section and enter an expression for filtering based on payload data in network packets of the selected network sessions.

     ```
     Filtering expression example
     ```

     ```
     ^test.+xABxCD
     ```
5. Click **Download**.
6. If it takes a long time (more than 15 seconds) to create the file, the file creation operation is transferred to the list of background operations. In this case, to download the file:

   a. Click the button in the menu of the application web interface.

      The list of background operations appears.

b. Wait for the file generation operation to complete.

c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Monitoring events and incidents

When analyzing industrial network traffic, the application registers events and incidents.

An *event* in Kaspersky Industrial CyberSecurity for Networks is an entry containing information about the detection of certain changes or conditions in industrial network traffic requiring the attention of an ICS security officer. Events are registered and transmitted to the Kaspersky Industrial CyberSecurity for Networks Server. The Server processes received events and saves them in a database.

An *incident* is a special type of event that is registered when a certain sequence of events is received. Incidents group events that have certain common traits or that are associated with the same process.

The application registers incidents based on event correlation rules. An *event correlation rule* describes the conditions for checking the sequences of events. When the application detects a sequence of events matching the rule conditions, it registers an incident that indicates the name of the triggered rule. Incidents are registered using the system event type that is assigned the code 8000000001.

Event correlation rules are embedded in the application and are applied regardless of the security policy.

After installation, the application uses the default event correlation rules. To improve the effectiveness of rules, Kaspersky experts regularly update the databases containing the sets of rules. You can update correlation rules by installing updates.

The Kaspersky Industrial CyberSecurity for Networks Server registers events and incidents according to the settings defined for registering event types. You can configure these settings in the Event types section (for all event types) and when configuring Process Control rules (only for events that are registered when Process Control rules are triggered).

To reduce the number of frequently recurring events that do not require attention from the operator, you can create allow rules for events. Events that satisfy allow rules are not registered. For example, you can use an allow rule to temporarily disable registration of all events from a specific monitoring point. You can view allow rules for events in the **Allow rules** section. The EVT type is indicated for these rules.

The application saves events and incidents in the database on the Server. The total volume of saved entries cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. If the minimum storage time limit is enabled and the application deletes entries whose storage time is less than the defined limit, a corresponding message will appear in the application message log. You can configure the settings for storing events and incidents.

Database files are saved on the Server in the DBMS folders. Deleting or modifying any file in these folders may cause a disruption in application performance.

You can view information about events and incidents in the following sections of the Kaspersky Industrial CyberSecurity for Networks web interface:

- The **Dashboard** section displays general information about the latest events and incidents registered by the application.
- The **Events and incidents** tab of the **Events** section displays detailed information about events and incidents and allows downloading information from the Server database for any period.

Scores and severities of events

Events and incidents in Kaspersky Industrial CyberSecurity for Networks are scored on a scale from 0.0 to 10.0.

If an event is linked to a device, the application calculates a numerical value for the score based on available information about the device. When calculating a score in this case, the application considers the level of importance of the device and the risks associated with this device.

The starting value used for calculating the score is the *base score* defined for the specific type of event in the event types table or defined when configuring Process Control rules (only for events that are registered when Process Control rules are triggered).

If an event is not linked to a device, the score of this event is equal to the base score.

This score determines the event severity level. Depending on the numerical value of its score, an event can have one of the following severities:

- *Low* (scores 0.0–3.9)

  Low-severity events normally do not require an immediate response.

- *Medium* (scores 4.0–7.9)

  Medium-severity events contain information that requires attention. These events may require a response.

- *High* (scores 8.0–10.0)

  High-severity events contain information that may have a critical impact on the industrial process. These events require an immediate response.

To ensure compatibility with the *severity levels* of events that were used in previous versions of the application, the current version of Kaspersky Industrial CyberSecurity for Networks converts those severity levels into the following scores:

- Events with *Informational* severity are assigned a score of 3.0.
- Events with *Warning* severity are assigned a score of 6.0.
- Events with *Critical* severity are assigned a score of 9.0.

Event registration technologies

Kaspersky Industrial CyberSecurity for Networks registers events based on one of the following technologies:

- *Deep Packet Inspection* (DPI)

  This technology is used to register events associated with process violations (for example, an event where the specified temperature was exceeded).

- *Network Integrity Control* (NIC)

  This technology is used to register events associated with industrial network integrity or the security of communications (for example, an event for the detection of communications between devices in the industrial network over a protocol that is new for those devices).

- *Intrusion Detection* (IDS)

  This technology is used to register events associated with the detection of traffic anomalies that are signs of an attack (for example, an event for the detection of signs of ARP spoofing).

- *Command Control* (CC)

  This technology is used to register events associated with the detection of system commands for devices in traffic (for example, an event for the detection of an unauthorized system command).

- *External* (EXT)

  This technology is used for incidents and events that are received by Kaspersky Industrial CyberSecurity for Networks from recipient systems using Kaspersky Industrial CyberSecurity for Networks API methods.

- *Asset Management* (AM)

  This technology is used to register events associated with the detection of device information in traffic or in data received from EPP applications (for example, an event for the detection of a new IP address for a device).

- *Endpoint Protection Platform* (EPP)

  This technology is used to register events associated with threats detected by Kaspersky applications that perform functions to protect workstations and servers (for example, a malware detection event).

Event statuses

Statuses of events and incidents enable the application to show the progression of information processing by the ICS security officer.

The following statuses can be assigned to events and incidents:

- *New*

  This status is assigned to all events and incidents when they are registered in Kaspersky Industrial CyberSecurity for Networks.

- *In progress*

  You can assign this status to events and incidents that are currently being processed (in progress), for example, when investigating the reasons for registration of these events and incidents.

- *Resolved*

  You can assign this status to events and incidents that have already been processed (for example, investigation of the reasons for their registration is complete).

  > Events and incidents with a status of *Resolved* assigned to them are not taken into account by the application when determining the security states of devices displayed in the table of devices and on the network interaction map.

The statuses of events and incidents are changed manually. You can sequentially assign statuses in the order from *New* to *Resolved* (however, you are not required to assign an intermediate *In progress* status). After the status of an event or incident is changed, you cannot assign the previous status to it.

Table of registered events

You can view the table of registered events and incidents on the **Events and incidents** tab in the **Events** section.

By default, the table of registered events and incidents is updated in real time. The beginning of the table displays the events and incidents with the latest dates and times when last visible.

> The date and time when the event or incident was last visible may differ from the date and time of its registration (the date and time of registration is displayed in the **Start** column). For an event, the date and time when last visible may be updated during the event regeneration period for this type of event. For an incident, the date and time when last visible is updated according to the date and time of last occurrence of the events that are part of the incident.

The settings of events and incidents are displayed in the following columns of the table:

- **Start**

  For an event that is not an incident – date and time of event registration. For an incident – date and time of registration of the first event included in the incident. In the table, you can view the date together with the time, or just the date or time by itself. To choose the information to display, select the check boxes opposite the **Date** and/or **Time** settings.

- **Last seen**

  For an event that is not an incident, this is the date and time when the event last occurred. It may contain the date and time of event registration, or the date and time when the event regenerate counter value increased if the conditions for event registration were repeated during the event regenerate timeout. The value of the regenerate counter is displayed in the **Total appearances** column. For an incident, this is the latest date and time of last occurrence of events that are part of the incident. Just like with the **Start** column, you can view the date together with the time, or just the date or time by itself.

- **Title**

  Header defined for the event type.

- **Score**

Calculated value for the event score. Event severity level is designated by a numerical score. Depending on the severity, the score may have one of the following colors:

- Red designates an event with *High* severity.
- Yellow designates an event with *Medium* severity.
- Blue designates an event with *Low* severity.

- **Source**

  Address of the source of network packets. You can use the following settings to show or hide addresses and ports (abbreviations for table cells are listed in parentheses): **IP address**, **Port number (P)**, **MAC address**, **VLAN ID (VID)**, **Application-level address**. If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the table of devices.

- **Destination**

  Address of the destination of network packets. The display of address information can be configured the same way as the **Source** column.

- **Protocol**

  Application layer protocol that was being monitored when the application registered the event.

- **Technology**

  This icon corresponds to the technology that was used to register the event.

- **Total appearances**

  For an event that is not an incident, this is the value of the regenerate counter after the event is registered within the event regenerate timeout. A value greater than 1 means that the conditions for event registration were repeated N – 1 times. The value 1 is displayed for the incident in this column.

- **ID**

  Unique ID of the registered event or incident.

- **Application**

  Information about applications that were running when event registration conditions occurred. An event saves the application data received from EPP applications.

- **Application user**

  Information about the user account that was used to start the application specified in the **Application** column.

- **Status**

  This icon corresponds to the status of an event or incident.

- **Description**

  Description specified for the event type.

- **End**

  For an event that is not an incident, this is the date and time when the *Resolved* status was assigned, or the date and time of the event regenerate timeout. For an incident, this is the latest date and time of the end of events that are part of the incident. Just like with the **Start** column, you can view the date together with the time, or just the date or time by itself.

- **Triggered rule**

  For an event that is not an incident, this is the name of the Process Control rule or Intrusion Detection rule whose triggering caused the registration of the event. For an incident, this is the name of the correlation rule whose triggering caused the registration of the incident.

- **Monitoring point**

  Monitoring point whose traffic invoked registration of the event.

- **Event type**

  Numerical code assigned to the event type.

- **Marker**

  This is a selection of icons that you can set for any event or incident so that you can easily find events and incidents based on a criterion that is not in the table.

When viewing the table of events and incidents, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing events included in an incident

For viewing events included in incidents, the following modes are provided in the table of events:

- Simple viewing mode. In this mode, the table of events displays all events without consideration of how events are nested in incidents.

- Tree display mode. In this mode, incidents are displayed as tree structures that can be collapsed or expanded using the and buttons next to the headers of incidents.

You can change the display mode when configuring the table of events.

Viewing event details

Detailed information about events and incidents is displayed in the details area in the **Events** section of the application web interface.

To view the details of an event or incident:

On the **Events and incidents** tab in the **Events** section, select the relevant event or incident.

The right part of the web interface window will show the details area, which displays detailed information about the selected event or incident.

Changing the statuses of events

You can change the following statuses of events and incidents:

- *New*. This status can be changed to *In progress* or *Resolved*.
- *In progress*. This status can be changed to *Resolved*.

A status of *Resolved* cannot be changed.

If an event is associated with a risk, you can change the risk status to *Accepted* when assigning a status of *Resolved* to this event.

To change the status of events or incidents when working with the table of events:

1. Select the **Events and incidents** tab in the **Events** section.
2. In the table of events, select the events and/or incidents whose status you want to change.
3. Open the **Change status** drop-down list in the toolbar.
4. In the drop-down list, select the command to assign the required status.

   Some drop-down list items are not available in the following cases:

   - The **In progress** item is unavailable if the selected items do not include events or incidents with a status of *New*.
   - The **Resolved** item is unavailable if the selected items do not include events or incidents with a status of *New* or *In progress*.

   > If all events and incidents that satisfy the current filter and search settings are selected, and the number of selected items is more than 1000, the application does not check their statuses. In this case, the **In progress** and **Resolved** items are both available. However, the **In progress** item can be used to assign a status of *In progress* only to events and incidents that have a status of *New*.

   A window with a confirmation prompt opens.
5. If the selected events are associated with risks and you want to simultaneously assign the *Accepted* status to these risks, select the **Assign the Accepted status for risks related to the event** (if one event is selected) or the **Assign the Accepted status for risks related to the events** (if multiple events are selected).

   Risks may be associated with events when the application registers events of certain types based on Asset Management technology.
6. In the prompt window, click **OK**.

Viewing details of EDR incidents

EPP events may contain information on the threat development chains received from the Endpoint Agent software components. If a threat development chain is built for an event, Kaspersky Industrial CyberSecurity for Networks considers such event an *Endpoint Detection and Response* incident (EDR incident).

A threat development chain is a sequence of activity events on a device associated with a detected threat. A key activity event in the threat development chain is an activity event with a threat detection object. All other activity events in the chain (preceding and following the key activity event) are saved for further threat development analysis.

Information on the threat development chain built may not be added to the event simultaneously with the registration of this event. The maximum delay in adding this information to an event by the application is 10 hours after its registration. The information is not added if the event has the *Resolved* status.

EDR incidents are marked with the **EDR** icon in the event table. For each EDR incident, you can view information on the threat development chain in the details area. The information is displayed on the following tabs in the details area:

- **Activity event graph** provides visual information about objects involved in the threat development chain. Activity events are represented as nodes on the graph. The nodes are located at different levels in accordance with the identified threat development process. The key activity event is located at the lowest level of the graph. This level can also display nodes that group other activity events by their types. Above this level, the application can display up to four levels with activity event nodes.

- **All activity events** displays table view of the information about all activity events included in the threat development chain and presented as nodes in the activity event graph.

When viewing the details of an EDR incident, you can determine the potential threat status by looking at the detection processing status. The application displays this status for the threat development chain. The background color for the status depends on the result of the threat detection object processing:

- If a detected threat is considered eliminated after being processed (for example, an infected object has been disinfected by an EPP application), the application displays the detection processing status on a green background;

- In all other cases, the detection processing status is displayed on a red background.

A key activity event in the activity event graph has the same color as the detection processing status.

If the detection processing status is displayed on a red background, you can prevent further development of a possible threat, for example, by triggering a response action in Kaspersky Industrial CyberSecurity for Networks.

Under any circumstances and regardless of the displayed detection processing status, you must investigate the causes and possible consequences of an EDR incident that has occurred.

You can view detailed information on activity events in the details windows that open when you select activity events. When viewing the details, you can use links with file and URL hashes to obtain information on the reputation of these objects on the Kaspersky Threat Intelligence Portal.

If the threat development chain contains activity events that you want to detect during the next checks of EPP applications, you can export the data on these activity events to an IOC file (an indicator of compromise file).

Creating allow rules for events

If you need to disable registration of events with specific indicators (for example, all events from a monitoring point), you can create allow rules for events. This section contains instructions on creating allow rules for events.

Users with any role except the Operator role can create allow rules for events.

Creating an allow rule with blank settings or settings from a template

To create an allow rule with blank settings or settings from a template:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, open the details area by clicking **Add rule**.

3. If you want to define the values of settings from a template, in the details area click **Use template**, select the necessary template in the opened window and click **Apply**.

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

5. In the **Protocol** field, specify the protocol that will be indicated in the events.

   When the **Protocol** field is selected, a window opens showing the table of supported protocols displayed as a protocol stack tree. You can manage how tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   If necessary, use the search field above the table to find relevant protocols.

   To specify the protocol:

   a. In the protocols table, select the protocol that you want to specify for the rule. To select the relevant protocol, click the button that is displayed in the left column of the protocols table.

   b. Click **OK**.

   If you select a protocol that can be identified by the application based on the contents of network packets, a notification about this appears below the **Protocol** field.

6. If required, enter additional information about the rule in the **Comment** field.

7. In the **Side 1** and **Side 2** settings groups, specify the editable address information for the participants (sides) of network interaction. Depending on the selected protocol (or set of protocols), address information may contain a MAC address, IP address, and/or port number. If additional address spaces were added to the application, you can specify the names of the address spaces for addresses.

To autofill the address information of a side of network interaction, you can select devices that are known to the application. To do so:

a. Open the device selection window by clicking **Specify device addresses**.

b. In the device selection window, select the check boxes next to the devices that you want to use.

The device selection window contains a table in which you can configure the layout and order of columns, and also filter, search, and sort similarly to the table of devices in the **Assets** section.

c. Click **OK** in the device selection window.

8. In the **Event type** field, specify the event type whose numerical code is indicated in events.

Selecting the **Event type** field opens a window containing a list of event types that may be indicated in allow rules. If necessary, use the search field above the list to find the relevant event type. To specify the event type, select it in the list and click **Apply**.

9. In the **Monitoring point** field, specify the monitoring point name that is indicated in events.

Selecting the **Monitoring point** field opens a window containing a list of all monitoring points on all nodes that have application components installed. If necessary, use the search field above the list to find the name of the relevant monitoring point. To specify the monitoring point name, select it in the list and click **Apply**.

10. In the **Rule in event** field, enter the name (or part of the name) that is indicated as the triggered rule in events.

11. In the details area, click **Save**.

The new rule will be added to the allow rules table.

Creating an allow rule from an existing one

To create an allow rule from an existing one:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

This action can be performed by a user with any role except the Operator role.

2. In the **Allow rules** section, select the rule that you want to use as the basis for creating a new rule.

3. Right-click to open the context menu.

4. In the context menu, select **Copy rule**.

The details area in rule editing mode will appear in the right part of the web interface window. The settings of the new rule will take the values obtained from settings of the selected rule.

5. Change the settings as necessary. To do so, complete steps 4–11 described in the procedure for creating a rule with initially empty values of settings.

Creating an allow rule from a registered event

To create an allow rule from a registered event:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Select the **Events and incidents** tab in the **Events** section.

3. In the table of registered events, select the event that you want to use as the basis for creating the allow rule for events.

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

4. In the details area, click **Create allow rule**.

   The **Allow rules** section opens in the browser window. The details area in rule editing mode will appear in the right part of the web interface window. The new rule's settings will take the values received from the saved information about the event.

5. If necessary, edit the settings of the new rule. To do so, complete steps 4–11 described in the procedure for creating a rule with initially empty values of settings. If you do not need to change the settings of the new rule, save the rule by clicking **Save**.

Setting markers

You can assign specific markers to events and incidents in the **Events** section of the application web interface.

A *marker* is an icon that lets you easily find events and incidents based on a criterion that is absent from the table.

To set a marker for an event or incident:

1. On the **Events and incidents** tab in the **Events** section, left-click to open the context menu in the cell of the **Marker** column for the row containing the relevant event or incident.

2. In the context menu, select the marker that you want to set for this event or incident.

   You can select one of the seven markers provided in the application. You choose the purpose of each marker on your own.

3. If you need to remove a marker, select **No marker** in the context menu.

Copying events to a text editor

You can copy information about the events and incidents displayed in the table of events to any text editor. The information is copied from the columns that are currently displayed in the table.

The capability to copy is available if no more than 200 events and incidents are selected.

To copy events and/or incidents to a text editor:

1. Select the **Events and incidents** tab in the **Events** section.
2. In the table of events, select the events and/or incidents whose information you want to copy to a text editor.
3. Right-click to display the context menu of one of the selected events.
4. In the context menu, select one of the following options:
   - **Copy details of the event** if one event or incident is selected.
   - **Copy details of the selected events** if multiple events and/or incidents are selected.
5. Open any text editor.
6. Paste it into the text editor window (for example, by pressing the key combination **CTRL+V**).

The copied event details can be edited in the text editor. Information about multiple events will be separated by an empty line.

Loading traffic for events

When viewing the table of events, 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 table of events (including events within incidents).

Traffic for events is loaded from the application database. The database saves traffic only when registering events for which traffic saving is enabled. The application can also save traffic in the database directly by requesting to load traffic using traffic dump files. These files are intended for temporarily saving traffic and are automatically deleted as more and more traffic is received from the industrial network (the frequency of file deletion depends on the amount of traffic received and the defined application data storage settings). To ensure that traffic is loaded, it is recommended to enable the saving of traffic for the relevant event types and configure the settings for saving traffic in the database in accordance with the rate of traffic and registration of events.

To load a traffic file for events and/or incidents:

1. On the **Events and incidents** in the **Events** section, select the events and/or incidents for which you want to download traffic.
2. Click **Download traffic**.
3. If file generation takes a long time (more than 15 seconds), the operation is moved to the background. If this is the case, follow these steps to download the file:
   a. Click in the application web interface menu.

      The list of background operations opens.

b. Wait for the file generation operation to complete.

c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Exporting activity event data into a file of indicators of compromise

When viewing details of EDR incidents, you can export data on activity events to an IOC file if you wish to detect such activity events during the next checks of EPP applications. For example, you can use the received IOC file in IOC search tasks performed using the Endpoint Agent software component.

To export activity event data to an IOC file:

1. On the **Events and incidents** tab in the **Events** section, select an EDR incident (the event marked with the **EDR** icon) that contains a threat development chain with the appropriate activity events.

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

2. In the details area, go to the **All activity events** tab and select the appropriate activity events.

   You can select activity events of the following types: **File creation**, **Starting a process**, or **Registry change**.

3. Click **Export to IOC file**.

4. In the window that opens, select a condition for detecting indicators of compromise:

   - **OR (any IOC detected)** if you want the IOC search task to be triggered when any indicator of compromise from the IOC file is detected.

   - **AND (all IOCs detected)** if you want the IOC search task to be triggered when all indicators of compromise from the IOC file are detected.

5. View the information that will be exported to the IOC file.

   Export is only available if non-zero values of the counters are displayed for any of the **File creation**, **Starting a process**, and **Registry change** fields. The field **Non-exportable** contains the number of selected activity events whose data cannot be exported to an IOC file.

6. Click **Export**.

7. If file generation takes a long time (more than 15 seconds), the operation is moved to the background. If this is the case, follow these steps to download the file:

   a. Click in the application web interface menu.

      The list of background operations opens.

   b. Wait for the file generation operation to complete.

   c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Creating a folder for exporting events to a network resource

You can export events and save a file with the exported events on a network resource of the Server computer. You can share a network resource by using the Network File System (NFS) protocol, which is employed to mount a shared network resource of another computer (such as an NFS server export point) in the local file system of the Server computer. The standard tools of the operating system can be used to create a folder and to mount a shared network resource.

When using the NFS protocol, the rpcbind software package is activated in the operating system. Please keep in mind that cybercriminals may attempt to use this software package to conduct certain types of DDoS attacks. To eliminate an infiltration threat, the firewall must be properly configured. In the CentOS Stream operating system, you are advised to use the network security configuration application known as Firewalld.

Manually creating a folder and mounting a shared network resource

To create a folder for saving files to a network resource:

1. Open the operating system console.
2. Create a local folder for mounting the shared network resource. To do so, enter the following command:

```
mkdir <full path of the local directory>
```

Example

```
mkdir ~/nfsshare
```

3. After the folder is created, enter the following command for mounting a network resource:

```
sudo mount -t nfs <remote computer name or IP address>:<full path of the shared network resource> <full path of the local directory>
```

Example

```
sudo mount -t nfs nfs-server.example:/nfsshare ~/nfsshare
```

4. Check the mount result by using the following command:

```
mount | grep <full path of the local directory>
```

Example

```
mount | grep ~/nfsshare
```

If mounting was successful, you will see data containing the name or IP address of the remote computer, the name of the shared network resource, and the name of the parent folder.

Automatically mounting a shared network resource

To configure automatic mounting of a shared resource in the CentOS operating system:

Open the /etc/fstab file for editing with root privileges and add the following string to the text of the file:

```
<name or IP address of the remote computer>:<full path of the shared network resource> <full path of the local directory> nfs defaults 0 0
```

Example

```
nfs-server.example:/nfsshare /home/user1/nfsshare nfs defaults 0 0
```

Monitoring risks

Kaspersky Industrial CyberSecurity for Networks can detect risks that could affect resources of an information system. The application detects risks based on traffic analysis and received information on devices.

The detected risks may belong to the following categories:

- Vulnerability. This category includes detected vulnerabilities of devices.
- Configuration problems. This category includes risks affecting the secure operation of devices due to incorrect configurations and risks of data compromise when writing and reading configurations of devices.
- ICS security breach. This category includes risks of information security breaches in automated industrial control systems.
- Insecure network architecture. This category includes risks associated with the detection of insecure network interactions, devices, protocols, and software, risks from inactivity of authorized devices, and risks from the absence or improper operation of EPP applications on devices.

Each risk is scored on a scale from 0.0 to 10.0. The application calculates this numeric risk score value based on the available information about the device associated with the detected risk. When calculating a risk score, the application considers the level of importance of the device, and other risks associated with this device. A *base score* is used as the initial value for calculations. Base scores of risks in the Vulnerability category are determined according to the Common Vulnerability Scoring System (CVSS). All other risk categories utilize the base scores defined in the table of risk types.

Information about risks is uploaded to the database of detected risks on the Kaspersky Industrial CyberSecurity for Networks Server. The total volume of saved entries in the database cannot exceed the defined limit. If the volume exceeds the defined limit, the application automatically deletes 10% of the oldest entries. You can set a maximum volume limit for detected risks when configuring data storage settings on the Server node.

The contents of the database of detected risks are displayed in the **Risks** section of the application web interface. You can also view general information about the risks associated with devices in the **Assets** section on the **Devices** tab.

About risks in the Vulnerability category

Vulnerability risks are registered when the application detects vulnerabilities in monitored industrial network devices. A *vulnerability* is a defect or flaw in device hardware or software that a hacker could exploit to impact the operation of an information system or to gain unauthorized access to information.

The application detects vulnerabilities by analyzing available information about devices. The relevant information utilized to find a known vulnerability of a device is compared to specific fields in the *database of known vulnerabilities*. The database of known vulnerabilities is built in to the application. This database is created by Kaspersky experts who fill it with information about the latest or most frequently encountered vulnerabilities of devices in industrial networks.

The database of known vulnerabilities contains descriptions of vulnerabilities and descriptions of the devices affected by these vulnerabilities. This database also contains system security recommendations in the form of text or links to publicly available resources. Descriptions and recommendations from various sources are uploaded to the database of known vulnerabilities. These sources may be the manufacturers of devices or software, or various organizations specializing in industrial security. Descriptions and recommendations in the database are provided in English.

After the application is installed, the initial preconfigured database of known vulnerabilities is used. You can keep the database up to date by installing updates.

Kaspersky Industrial CyberSecurity for Networks compares available device information with the specific fields in the database of known vulnerabilities that describe devices affected by vulnerabilities. To detect vulnerabilities, the application uses the following information about devices:

- **Hardware vendor**.
- **Hardware model**.
- **Hardware version**.
- **Software vendor**. If no software vendor data is detected in the device information, Kaspersky Industrial CyberSecurity for Networks uses the value of the **Hardware vendor** field.
- **Software name**. If no software name is detected in the device information, Kaspersky Industrial CyberSecurity for Networks uses the value of the **Hardware model** field.
- **Software version**.

In the database of known vulnerabilities, descriptions of devices are stored in the CPE (Common Platform Enumeration) language format. The application compares the available device information with these descriptions, automatically converting the information into the CPE language format.

For each vulnerability, the matching descriptions are provided in the details area of the risk in the **Matched CPE** section.

If the device information matches the corresponding fields in the database of known vulnerabilities, the application registers a Vulnerability risk and uploads information about the vulnerability to the database of detected risks.

The main parameter used to identify a vulnerability is its identification number in the list of Common Vulnerabilities and Exposures (CVE). This identification number is known as a *CVE ID*. If a vulnerability has not yet been assigned a CVE ID, it is identified by its identification number obtained from other publicly available resources containing vulnerability descriptions.

Kaspersky Industrial CyberSecurity for Networks lets you obtain the identifiers and links to vulnerability descriptions provided by the Russian Federal Service for Technical and Export Control (FSTEC) in the Information Security Threat Database (also known as the BDU). If downloaded vulnerability information contains this type of information from the FSTEC BDU, the application displays this information as its corresponding identifiers in the format BDU:<year>-<number>.

Scenario for implementing the continuous risk management process

Risk detection functionality lets you implement continuous (cyclical) management of risks in your information system. For risk management purposes, Kaspersky Industrial CyberSecurity for Networks provides information on detected risks that you can use to take the appropriate measures to eliminate or mitigate those risks.

The scenario for implementing the continuous risk management process consists of the following stages:

1. **Device inventory**

   This stage is implemented by using the device activity detection and device information detection methods (these methods must be enabled). During this stage, the application automatically detects new devices and updates the device information. If the industrial network contains devices that have not been detected automatically, you need to manually add them or import them from external projects.

   For all information that defines the classification and operating specifications of devices (such as information about the device model and software version), you must enable auto update in the settings of devices. If auto update of this information cannot be completed for some reason, this information should be manually updated.

2. **Risk detection through passive and active scanning**

   The application passively scans devices for risks, utilizing the available device information. The application also detects risks by analyzing network interactions in industrial network traffic. Risk detection is implemented using the risk detection method (this method must be enabled).

   You can also perform active polling of devices to quickly obtain information about these devices. When performing active polling of devices, you also can detect specific types of risks if the corresponding risk analysis methods are selected. To conduct active polling of devices, one or more **Active poll** connectors must be added to the application.

   Vulnerability risks are detected automatically after the application database of known vulnerabilities is updated or after adding or modifying device information used for comparison (for example, after the information about the device model and software version is saved).

3. **Assessment and classification of detected risks**

   The application calculates a score value for each detected risk. This score determines the severity level of the risk. Depending on its score, a risk may have a *Low* (score of 0.0–3.9), *Medium* (4.0–7.9), or *High* (8.0–10.0) severity.

   You can classify detected risks based on their severities and scores, and also on other factors related to the operational specifics of the devices used in your information system. If you assess a risk as negligible, its status can be manually changed from *Active* (assigned to a detected risk by default) to *Accepted*. For instance, this could be done if the conditions for exploiting a vulnerability cannot be reproduced anyway. When changing the status of a risk, it is recommended to add or edit the comment for the risk.

   All risks that require some additional actions should be left as *Active*.

4. **Risk mitigation**

   At this stage, you need to take actions that help either eliminate the detected risks or minimize the threats associated with the potential realization of these risks. To do so, check all detected risks with a status of *Active*, beginning with the risks that have the highest scores. Perform the necessary actions in your information system (for example, to eliminate a device vulnerability, install the required software update or isolate this device from external networks if the update is impossible). Information about recommended mitigation measures is provided for certain risks (such as vulnerabilities).

   > Remediation actions for detected risks are performed without the involvement of Kaspersky Industrial CyberSecurity for Networks.

5. **Verification of risk mitigation**

   This stage is similar to risk detection through scanning. When this stage is completed, the table of risks should no longer have any *Active* risks.

   Most risks detected by the application during passive scanning (such as vulnerabilities) are automatically assigned a status of *Remediated* if the conditions under which these risks were detected are no longer met. For example, after the version of software on a device is changed, the application assigns a status of *Remediated* to a Vulnerability risk that had been registered due to a previous vulnerable version of the software. A status of *Remediated* is also assigned to risks that no longer have a description in the database of known vulnerabilities (for instance, if the description is deleted from the database after updates are uploaded).

   When deleting devices, the application also deletes the risks that were associated with these devices.

   If you have taken action to mitigate a risk but the risk detection conditions have not changed (for example, a vulnerable device has been isolated from external networks but the information about this device has not changed), you can manually assign a status of *Accepted* to this risk. When changing the status of a risk, it is recommended to add or edit the comment for the risk.

   Some risks cannot be automatically assigned a status of *Remediated* (for example, *Remediated* cannot be automatically assigned to risks that are detected during active polling of devices). For these types of risks, you also have to manually assign a status of *Accepted* after conducting risk mitigation measures.

   If a risk is associated with an event, you can assign a status of *Accepted* to this risk simultaneously while changing the event status to *Resolved*.

Viewing the risks table

The risks table is displayed in the **Risks** section of the application web interface.

The risk settings are displayed in the following columns of the table:

- **Category**

  Name of the risk category.

- **Name**

  Name of the risk. The CVE ID of the detected vulnerability is used for a Vulnerability risk (if it has no CVE ID, it is identified by its identification number obtained from other publicly available resources containing vulnerability descriptions).

- **CVE**

  For a Vulnerability risk: CVE ID of the detected vulnerability.

- **BDU**

  For a Vulnerability risk: vulnerability ID in the BDU database. If one vulnerability with a CVE ID matches multiple vulnerabilities with different IDs in the BDU database, this column contains all the IDs.

- **Risk ID**

  Unique ID of the risk.

- **Score**

  Calculated value of the risk assessment. The severity of the risk is designated by a numerical score. Depending on the severity, the score may have one of the following colors:

  - Red designates a *High* severity risk.
  - Yellow designates a *Medium* severity risk.
  - Blue designates a *Low* severity risk.

  For risks with a status of *Active*, the score is brightly colored. For *Remediated* or *Accepted* risks, the score is faintly colored.

  In the details area, this setting is referred to as **Base score**.

- **Side 1**

  Address information of one of the sides of network interaction (indicated for certain risk types). MAC addresses and IP addresses can be individually enabled and disabled. If additional address spaces were added to the application, you can enable or disable the display of the names of address spaces by using the **Show address spaces** setting when configuring the risks table.

- **Side 2**

  Address information of the other side of network interaction (indicated for certain risk types). The display of address information can be configured the same way as the **Side 1** column.

- **Device group**

  Name of the group containing the device with the detected risk (contains the name of the group and the names of all its parent groups).

- **Device**

  Device name and address.

- **Source**

  For a Vulnerability risk: name of the source of the information uploaded to the database of known vulnerabilities. In the details area, this setting is referred to as **Source of vulnerability**.

- **Status**

  Current status of the risk. The following statuses are available:

  - *Active* is the default status upon first detection of the risk (and upon repeated detection if a status of *Remediated* had been assigned to the risk). You can also manually assign a status of *Active* to a risk that is currently *Accepted*.
  - *Remediated* is the automatically assigned status if the conditions for risk detection are no longer present.
  - *Accepted* is the status manually assigned to a risk if the risk is assessed as negligible or if risk mitigation measures did not lead to automatic assignment of *Remediated*.

- **Detected at**

  Date and time of risk detection.

- **Last status change**

  Date and time of the last change of the risk status.

- **Matched CPE**

  For a Vulnerability risk: descriptions of devices from the database of known vulnerabilities. These are descriptions that match device information in the table of devices.

When viewing the risk table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Viewing risk details

Risk details include information from the table of risks and the following fields:

- **Risk type** – risk type code.
- **Description** – description defined for the risk type or the corresponding vulnerability.
- **Base score** – initial value used for calculating a numeric value for a risk score.

For a Vulnerability risk, additional information is displayed in the following fields and groups of fields:

- **CVSS vector** – record of metrics used to calculate a CVSS vulnerability score.
- **Attack conditions** – description of the vulnerability exploitation conditions.
- **Impact** – description of the potential effects from exploitation of the vulnerability.
- **Mitigations** – recommendations on remediating the vulnerability (for example, which software version should be installed on the device).
- **Links** – links to publicly available resources containing additional information about the vulnerability.
- **CVE history** – dates of identification, confirmation, and publication of the vulnerability in publicly available sources.

To view information about a risk:

Select the relevant risk in the table of risks.

In the right part of the web interface window, you will see the area containing detailed information about the risk.

*To view the details of a Vulnerability risk on the **Devices** tab in the **Assets** section:*

Click the name of the vulnerability (displayed as a CVE ID or other identification number of the vulnerability) in the **Risks** column or in the details area of a device with this risk.

You will see a window containing detailed information about the vulnerability.

Manually changing the statuses of risks

When working in the **Risks** section, you can manually change the statuses of any risks from *Active* to *Accepted* and vice versa. When working in the **Assets** section, you can change the status only for Vulnerability risks and only from *Active* to *Accepted*.

You can also assign a status of *Accepted* to a risk when assigning *Resolved* to events that are associated with this risk.

To manually change the status of a risk:

1. Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface under a user account that has been assigned a role with the access rights to perform this action.

   This action can be performed by a user with any role except the Operator role.

2. Open the risk details area or the window containing detailed information about the risk.

3. Open the **Change status** drop-down list.

4. Depending on the status you want to assign to the risk, select one of the following items in the drop-down list:

   - **Accepted** – if you want to change the risk status from *Active* to *Accepted*.
   - **Active** – if you want to revert the risk back to the *Active* status.

   A window with a confirmation prompt opens.

5. If events are associated with the selected risk and you want to simultaneously assign a status of *Resolved* to all these events, select the **Assign the Resolved status to all related events** check box.

   Risks may be associated with events when the application registers events of certain types based on Asset Management technology.

6. In the prompt window, click **OK**.

Viewing risk details when working with the table of devices

When working with the table of devices you can view information about the risks that were detected on devices. The names of detected vulnerabilities (identified as CVE IDs or other identification numbers of the vulnerabilities) are displayed for each device that contains Vulnerability risks. If risks of other categories were detected on a device, the names of these risk categories are displayed for this device. The names of vulnerabilities and risk categories are displayed in the **Risks** column and in the details area when a device is selected.

By default, the table of devices displays information only for the risks that are assigned a status of *Active*. If necessary, you can enable the display of information about all risks by selecting **Show remediated and accepted risks** when configuring the table of devices.

To designate the severity levels of risks, the names of vulnerabilities and categories are displayed in one of the following colors:

- Red designates *High* severity risks.
- Yellow designates *Medium* severity risks.
- Blue designates *Low* severity risks.

For risks with a status of *Active*, the names are brightly colored. For risks with a status of *Remediated* or *Accepted*, the names are faintly colored.

If risks of the same category are associated with a device, the name of this category is shown in the color of the highest severity level of all these risks.

If you want to view detailed information about risks, you can use the displayed names of vulnerabilities and risk categories. Click the name of a vulnerability (displayed as a CVE ID or other identification number of the vulnerability) to open the details window of the vulnerability. When you click the name of a risk category, the application switches to the risks table and applies a filter to display risks of the selected category that are associated with the device.

When viewing the table of devices, you can configure the settings for filtering devices based on their associated risks. You can also search for devices based on the names of their vulnerabilities (identified as CVE IDs or other identification numbers of the vulnerabilities).

Deep Packet Inspection

Kaspersky Industrial CyberSecurity for Networks lets you monitor an industrial process by providing you with information about the process parameters and system commands transmitted in industrial network traffic. The application tracks this data for devices that are displayed in the table of devices and that have defined Process Control settings.

You can view the monitored tags and existing Process Control rules on the Server web interface page in the **Process control** section. The Process Control settings for devices are available when you select the corresponding devices in the **Assets** section and **Network map** section.

Monitoring process parameter values

Kaspersky Industrial CyberSecurity for Networks can display the values of process parameters (tags) in real time.

To display these values, you must add the relevant tags to the application. You can add tags when configuring Process Control.

The application does not save the tag values displayed in real time. The names and values of tags may be saved in events registered based on Deep Packet Inspection technology (the tag values received when the event is registered are saved in the event). To save the names and values of tags, the variable $tags must be present in the settings of event types.

To view the values of process parameters:

Connect to the Kaspersky Industrial CyberSecurity for Networks Server via the web interface and select the **Tags** tab in the **Process control** section.

The browser window will display a table containing the tags and their current values. The following tag parameters show values that are modified on the fly:

- **Basic data type**
- **Read/write**
- **Received**
- **Timestamp**
- **Timestamp status**
- **Data status**
- **Originator**
- **Value**
- **Structural values**
- **Cause of transmission**

To monitor the values of tags, you can utilize all the functions that are available when viewing the table of tags.

Settings of tags

The settings of tags utilized for process control are displayed in the table of tags and in the details area when a tag is selected.

Depending on the columns selected for display, the table of tags may show the following settings:

- **Device group** – name of the group containing the device associated with the tag (contains the name of the group and the names of all its parent groups in the device group tree). In the details area, this setting is referred to as **Group**.
- **Device** – name of the device associated with the tag.
- **Protocol** – name of the protocol used to transmit the tag.
- **Tag name** – defined name of the tag.
- **Protocol data type** – tag data type indicating a specific name for the protocol operation (if such names are supported in the protocol, for example, for IEC 60870-5-104 and IEC 60870-5-101 protocols) or denoted by a standard data type name (for example, int32).
- **Unit of measure** – unit of measurement for the process setting represented by the tag.

- **Basic data type** – data type for the value that is the primary value in the tag field structure (indicated by the standard data type name).
- **Read/write** – direction of transmission when a tag value was received (R when reading from the device, W when writing to a device, and RW for both directions).
- **Favorites** – indicator of whether the tag was added to the favorites list.
- **Description** – additional information about the tag.
- **Tag address** – hardware address of the tag in the device memory.
- **Tag ID** – sequential number of the tag. A tag ID is assigned automatically. In the details area, this setting is referred to as **ID**.
- **Received** – date and time when the tag value was last received by the application.
- **Timestamp** – date and time when the tag value (received from traffic) was last modified or updated.
- **Timestamp status** – status on the date and time when the tag value was last modified or updated.
- **Data status** – current status of the received tag value.
- **Originator** – name of the source from which the tag value was received or the command was sent.
- **Value** – tag value that is modified on the fly during operations.
- **Scalable tag** – indicator of tag scaling within the range of minimums and maximums for input and output values.
- **Input (minimum)** – minimum boundary of the input value.
- **Input (maximum)** – maximum boundary of the input value.
- **Output (minimum)** – minimum boundary of the output value.
- **Output (maximum)** – maximum boundary of the output value.
- **Structural values**: a list of names and values for all tag fields List items are separated by a comma and space (for example: `field1: <value1>, field2: <value2>`). The names of nested fields are generated from the names of all parent fields and the name of the actual field, separated by colons (for example: `parent1:parent2:field: <value>`). String values must be enclosed in quotation marks.
- **Cause of transmission** – reason for modification or transmission of the tag value (received from traffic).
- **Source** – information about the source of tag creation. When the tag is created automatically, **Source** is set to **System**. If the tag is created or modified by a user, **Source** is set to **User**.

The details area for the selected tag may also display other settings determined by the device and protocol (for example, **Memory area**).

The types of frames comprising application service data units (ASDU) are supported for Deep Packet Inspection on devices that interact over protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards. For information on the supported ASDU types identification in these protocols, please refer to the Appendices.

Viewing the table of tags

The table of tags is displayed on the **Tags** tab in the **Process control** section. The table provides the general parameters of tags and of the devices associated with the tags.

When viewing the tag table, you can use configuration, filter, search, and sort functions, and navigate to the related items.

Detecting default passwords when connecting to devices

When monitoring the communications of process control devices, Kaspersky Industrial CyberSecurity for Networks can determine when default passwords are used. If a connection is made to a device using a password that is set as the default password for the particular class 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 classes 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

Devices	Protocols	System commands
Siemens SIMATIC S7-200, S7-300, S7-400	Siemens Industrial Ethernet Siemens S7comm	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ
Siemens SIMATIC S7-1200, S7-1500	Siemens Industrial Ethernet Siemens S7comm-plus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
PLC based on the CODESYS V3 platform (for example, Prosoft-Systems Regul R500)	CODESYS V3 Gateway	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD READ DEFAULT PASSWORD SET
EKRA 200 series	Modbus TCP for EKRA 200 series devices	DEFAULT PASSWORD READ DEFAULT PASSWORD SET
EKRA BE2502, BE2704 series	ABB SPA-Bus	DEFAULT PASSWORD ENTRY DEFAULT PASSWORD SET

To register default password detection events, the following conditions must be met:

- Interaction Control is enabled in monitoring mode and Command Control technology is applied.
- The allow rules table does not contain any rules for Command Control technology that allow system commands with default passwords. For example, the application may automatically create these rules in Interaction Control learning mode. If these rules are present in the allow rules table, you are advised to disable them.
- For the relevant devices, tracking of system commands with default passwords is enabled.

Obtaining reports

Using Kaspersky Industrial CyberSecurity for Networks, you can generate reports containing various information saved by the application. Kaspersky Industrial CyberSecurity for Networks generates report files in PDF format. The application can send the report files to the email addresses indicated by a user with the Administrator or Security Officer role. You can also download reports on the Server web interface page.

Kaspersky Industrial CyberSecurity for Networks supports the following types of reports:

- Reports based on templates.

  These reports contain accumulated information about the devices and their states, system security, monitored technological process parameters and system commands, and information about detected risks and interactions with third-party devices.

- Reports on vulnerability and compliance audit jobs.

  These reports contain information about the results of the vulnerability and compliance audit job runs.

You can view information about generated reports and export them to files on the **Generated reports** tab in the **Reports** section.

Viewing the reports table

You can view the reports table in the **Reports** section on the **Generated reports** tab of the application web interface.

The report settings are displayed in the following columns of the table:

- **ID**

  Unique identifier of the report.

- **Report name**

  Name of the generated report.

- **Template name**

  Name of the template used to generate the report.

- **Run**

  Date and time when report generation was started.

- **Status**

  Report completion status. The following report completion statuses are provided:

  - **Pending**. The report is in the creation queue. A report may have the *Pending* status when multiple reports are being generated at the same time.
  - **In progress**. The report is currently being generated.
  - **Error**. An error occurred when generating the report.
  - **Done**. Report generation is complete.
  - **Canceling**. Report generation is being canceled.
  - **Canceled**. Report generation was canceled.

- **User**

  Name of the user who started report generation or configured the schedule for generating a report based on a template.

- **Run type**

  Type of report generation launch: manually or as scheduled.

- **Completed**

  Date and time when report generation completed.

When viewing the reports table, you can use the configuration, filter, and sorting functions.

Exporting a report to a file

You can export a generated report to a file in PDF format.

To export a report to a file:

1. Select the **Reports** section.
2. On the **Generated reports** tab, select the relevant report.

Reports are filtered based on the IDs of reports that were last run in the current Server connection session. To display all generated reports, reset the filter settings by clicking **Default filter**. If necessary, you can configure filtering based on a specific period of time.

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

3. Click **Export**.

The browser will save the report file. By default, a report file is named according to the format `<report name>_<report generation date and time>`. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

Reports based on templates

Report templates in Kaspersky Industrial CyberSecurity for Networks can be of the following types:

- System templates are created automatically during installation of the application. In the report templates table, system templates are displayed with the icon. You cannot delete system templates.

  Kaspersky Industrial CyberSecurity for Networks supports the following system templates for generating reports:

  - **Inventory report**.

    Report containing information about devices, monitored technological process parameters and system commands, utilized protocols, and detected risks on devices.

  - **System security report**.

    Report containing information about the security status of devices, registered events, detected risks, and interactions with devices of external networks.

  - **Executive summary**

    Report containing concise information about devices and the security status of the system.

  - **Full report**

    Report containing comprehensive information about devices and the security status of the system.

- User-defined templates are created manually by duplicating templates. System templates and user-defined templates can be duplicated. Users with the Administrator or Security Officer role can duplicate templates.

Data in reports is presented in separate information blocks. For each report, Kaspersky Industrial CyberSecurity for Networks uses a fixed set and layout of information blocks. The information blocks used in reports and their descriptions are presented in the table below.

Use of information blocks in reports

Name of information block	Inventory report	System security report	Executive summary	Full report
Device categories	✓	—	✓	✓
Device vendors	✓	—	✓	✓
Device operating systems	✓	—	✓	✓
Monitored technological process parameters	✓	—	—	✓
Devices with the most risks	✓	✓	—	✓

Name of information block	Inventory report	System security report	Executive summary	Full report
Most vulnerable industrial devices	✓	✓	–	✓
System command sources	✓	–	–	✓
Situational awareness	–	✓	✓	✓
New devices in the network	✓	–	–	✓
Protocols with the most traffic	✓	–	–	✓
Devices with the most connections to other nodes	✓	–	–	✓
Network traffic volume	✓	–	✓	✓
Common protocols	✓	–	✓	✓
Industrial protocols	✓	–	✓	✓
System command recipients	✓	–	–	✓
Device security statuses	–	✓	✓	✓
Distribution of devices by status	–	✓	–	✓
Statistics on events	–	✓	–	✓
Distribution of events by detection technologies	–	✓	–	✓
Devices with the most events	–	✓	–	✓
Most critical events	–	✓	–	✓
Most frequently triggered malicious activity detection rules	–	✓	–	✓
Unusual protocols in the industrial network	–	✓	–	✓
Devices with signs of access to public resources	–	✓	–	✓
Connections via remote control protocols	–	✓	–	✓
Modification of industrial device programs	–	✓	–	✓
Active risks	–	✓	✓	✓

Viewing the report templates table

You can view the report templates table in the **Reports** section on the **Report templates** tab of the application web interface.

The settings of report templates are displayed in the following columns of the table:

- **Name**

  Report template name. The icon is displayed next to the names of system report templates.

- **Schedule**

  Information about the schedule used by Kaspersky Industrial CyberSecurity for Networks to automatically generate a report based on the template. Schedule information is displayed if a user with the Administrator or Security Officer role configured the schedule settings in the report template. If schedule settings were not defined, the column displays a value of **Off**.

- **Type/user**

  Name of the user who last modified the report template. **System** is displayed for system templates that have the default settings.

- **Last report**.

  Date and time when report generation was last started based on the report template.

- **Destinations**

  This icon indicates that there are email recipients of reports. The following icons are provided:

  - – report recipients are defined.
  - – report recipients are not defined.

When viewing the report templates table, you can use the configuration and sorting functions.

Viewing report template details

To view information about a report template:

On the **Report templates** tab in the **Reports** section, select the relevant template.

The details area appears in the right part of the web interface window. The details area displays all data that has defined values.

Report template details include the following fields:

- **Name** – report template name.
- **Type/user** – name of the user who last modified the report template. **System** is displayed for system templates that have the default settings.
- **Period** – time period covered when Kaspersky Industrial CyberSecurity for Networks generates a report based on the template.
- **Changed** – time of the most recent change to the template.
- **Last report** – time when the last report was generated based on the template.
- **Next run** – time when the next report generation will start based on the template. This setting is displayed if schedule settings were defined for the report template.

- **Schedule** –information about the schedule used by Kaspersky Industrial CyberSecurity for Networks to automatically generate a report based on the template. This setting is displayed if schedule settings were defined for the report template.

- **Destination addresses** – email addresses to which Kaspersky Industrial CyberSecurity for Networks sends the generated reports. This setting is displayed if recipient addresses were defined for the report template.

Generating a report based on a template manually

You can manually start report generation based on a template. Users with any role can manually start generating reports.

To start generating a report:

1. Select the **Reports** section.

2. On the **Report templates** tab, select one or more templates that you want to use to generate reports.

   When multiple templates are selected, the application simultaneously generates reports based on them. You can select no more than 10 templates.

3. Click **Get reports** in the toolbar located above the report templates table.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process. If necessary, you can contact a user with the Administrator or Security Officer role to cancel report generation.

You will be taken to the **Generated reports** tab, which will display the progress of the reports being generated. After the reports are generated, Kaspersky Industrial CyberSecurity for Networks sends the report files in PDF format to the email addresses indicated in the report template. If an email address is not defined in the report template, you can individually export generated reports to files manually on the **Generated reports** tab. The maximum size of a report file is 10 MB.

Reports on vulnerability and compliance audit jobs

Kaspersky Industrial CyberSecurity for Networks can generate reports with information about the results of the vulnerability and compliance audit jobs runs. A user with the Administrator or Security Officer role can configure automatic sending of reports by email. If necessary, you can manually generate a report for a completed job run or a completed device scan and then export the report to a file.

Generating a report on a manual job run

You can manually generate a report on the run of the vulnerability and compliance audit job. The report is generated based on the results of the scans performed on the devices using the vulnerability and compliance audit rules selected in the job settings.

The following reports on the vulnerability and compliance audit job runs are provided:

- **Full report**

  This report contains detailed information about the performed scans and the used vulnerability and compliance audit rules.

- **Executive summary**

  This report contains a summary of the most important scan results.

To generate a report, the vulnerability and compliance audit job run must have one of the following statuses: **Completed**, **Partially successful**, **Canceled**, or **Error**.

To start generating a report:

1. Select the **Security audit** section.
2. On the **Vulnerability and compliance audit** tab, select the job for which you want to generate the report.

   The details area appears in the right part of the web interface window.
3. In the details area, go to the **Runs** tab.
4. Select the desired job run.
5. In the job run details area that appears, open the **Get report** drop-down list and select the desired report: **Full report** or **Executive summary**. If the report cannot be generated, the drop-down list is not available.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process.

Go to the **Generated reports** tab in the **Reports** section. The vulnerability and compliance audit report appears in the table of generated reports. After successful report generation, you can export the generated report to a file.

Generating a report on a manual device scan

You can manually generate a device scan report within a vulnerability and compliance audit job. The report is generated based on the results of the scans performed on the device using the vulnerability and compliance audit rules selected in the job settings. The report contains detailed information about the performed scans and the used vulnerability and compliance audit rules.

To generate a report, the device scan must have one of the following statuses: **Completed**, **Canceled**, or **Error**.

To start generating a report:

1. Select the **Security audit** section.
2. On the **Vulnerability and compliance audit** tab, select the job within which the desired device scan is performed.

   The details area appears in the right part of the web interface window.
3. In the details area, go to the **Runs** tab.
4. Select the desired scan and click **Get report** in the scan details area that appears. The button is disabled if the report cannot be generated.

   Kaspersky Industrial CyberSecurity for Networks will start the report generation process.

Go to the **Generated reports** tab in the **Reports** section. The vulnerability and compliance audit report appears in the table of generated reports. After successful report generation, you can export the generated report to a file.

Detecting security issues in encryption protocols

If encryption protocols (such as SSL/TLS or SSH) are being used in an industrial network, Kaspersky Industrial CyberSecurity for Networks can detect various security issues in network interactions using these protocols. The application registers the appropriate event when detecting a security issue. The system event type for the detection of system commands is used to register these events.

The application registers events when it detects the following security issues in an encryption protocol:

- Use of an outdated version of an encryption protocol (DEPRECATED PROTOCOL VERSION).
- Use of a weak encryption algorithm (WEAK CIPHER TYPE).
- Use of an expired certificate (OUTDATED CERTIFICATE).
- Use of a self-signed certificate (SELF-SIGNED CERTIFICATE).

The list of detected security issues depends on the specific encryption protocol.

After installation, the application uses the original protocol processing modules that support a limited number of encryption protocols. You can update protocol processing modules by installing updates.

You do not need to add Process Control settings for devices to detect security issues in encryption protocols. The application analyzes the encryption protocols in all detected interactions.

To register security issue detection events, the following conditions must be met:

- Interaction Control is enabled in monitoring mode and Command Control technology is applied.
- The allow rules table does not contain any rules for Command Control technology that block the registration of events regarding security issues in encryption protocols. For example, the application may automatically create these rules in Interaction Control learning mode. If these rules are present in the allow rules table, you are advised to disable them.

Typical actions when working with data tables

This section contains information about the typical operations performed when working with the data tables that are displayed in different sections of the application web interface (such as the table of devices, table of events, or table of tags).

Viewing a data table

This section describes the features available when viewing data tables in the application web interface sections.

Configuring the columns display and order

Depending on the specific section of the application web interface, you can enable and disable the display of specific data in the table and configure which columns to display and in which order.

To configure the table display settings:

1. Click the icon to open the window for configuring how the table is displayed.
2. If enabling and disabling the display of specific data is available for the table (for example, display of remediated and accepted risks in the table of devices), configure the settings in the upper part of the window.
3. In the **Displayed columns** settings group, select the check boxes next to the settings that you want to view in the table. You must select at least one setting.
4. If you want to change the order in which columns are displayed, select the name of the column that needs to be moved to the left or right in the table and use the buttons containing an image of the up or down arrows.

The selected columns will be displayed in the table in the order you specified.

Filtering based on standard time periods

To filter the data table by standard time period:

1. When working with a table in a section of the application web interface, open the **Period**, **Run period**, or **Period** drop-down list in the toolbar.
2. In the drop-down list, select one of the standard periods (for example, **Last 24 hours**).

The table will display data for the period you specified.

Filtering based on a specified time period

To filter the data table by specified time period:

1. In a table of the application web interface section, in the toolbar, open the **Period**, **Period**, or **Run period** drop-down list.
2. In the drop-down list, select **Specify a period**.

   The start and end date and time of the filtering period are displayed on the right of the drop-down list.
3. Click the date of the start or end of the period.

   The calendar opens.

4. In the calendar, specify the date for the start and end boundaries of the filtering period. To do so, select a date in the calendar (the current time will be indicated) or manually enter the value in the format DD-MM-YYYY hh:mm:ss. If you do not need to specify the date and time of the filtering period end boundary, you can choose not to select a date or you can delete the current value.

5. Click **OK**.

The table will display data for the period you specified.

Filtering by columns

To filter a table by a specific column:

1. In a table of a section of the application web interface, click the filtering icon in the relevant column.

   The filtering window opens.

2. Use the interface elements in the filter window to configure the settings, as necessary. Below are some special considerations when configuring a filter in certain columns.

3. Click **OK**.

If the filter window contains the **Complex** field

Use the **Complex** field to specify multiple values combined by the logical operator AND. To add different types of values, click **Add condition (AND)**.

If there is a column for groups of devices

1. In the filter window, click the icon in the right part of the field to select a group.

   The **Select group in tree** window appears.

2. In the device group tree, select the relevant group and click **Select**.

   The path to the selected group is displayed in the field in the filter window.

If there is a column for risks associated with devices

1. In the filter window, use the **Exclude devices with risks** toggle switch to configure the display of devices in the table:

   - To view only risk-free devices, turn on the toggle button.
   - To view the devices with risks and to configure the settings for filtering by risk, turn off the toggle button.

2. If necessary, use the following controls to configure the settings for filtering devices with risks:

   - **Risk score** – lets you define a range of risk score values for displaying devices with risks whose scores are within the specified range.

   - **Status** – lets you enable and disable filtering based on the statuses of risks (corresponding buttons are displayed if **Show remediated and accepted risks** is selected in the table of devices display settings).

If there is a **Protocol** column with display of the supported application protocols

1. In the filter window, specify the necessary protocol in the **Protocols** field. To do so, start entering the name of the protocol and select the relevant protocol from the drop-down list (the list of suitable protocols is automatically expanded when the value in the **Protocols** field is changed).

2. If required, sort the opened list of protocols by clicking **Sort**.

3. If you want to add another protocol, click **Add protocol** and specify the other protocol in the field that opens.

4. If you want to delete one of the specified protocols, click the icon in the filter window. You can also delete all specified protocols by clicking **Default filter** in the filtering window.

If there is a **Protocol** column that displays all supported protocols in the form of a protocol stack tree

1. In the filter window, configure how the relevant tree elements are displayed by using the **+** and **-** buttons next to the names of protocols that contain protocols of subsequent layers.

   The table columns provide the following information:

   - **Protocol** – name of the protocol within the protocol stack tree.

   - **EtherType** – number of the next-level protocol within the Ethernet protocol (if the protocol has a defined number). It is displayed in decimal format.

   - **IP number** – number of the next-level protocol within the IP protocol (if the protocol has a defined number). It is indicated only for protocols within the IP protocol structure. It is displayed in decimal format.

2. If necessary, use the search field above the table to find relevant protocols.

3. In the list of protocols, select the check boxes opposite the protocols by which you want to filter events.

   If you select or clear the check box for a protocol that contains nested protocols, the check boxes for the nested protocols are also automatically selected or cleared.

If filtering based on the table cell values is allowed

1. Select the relevant items in the data table.
2. Move your mouse cursor over a cell of the relevant column of one of the selected items.
3. Right-click to open the context menu.
4. In the context menu, select the command that shows all items containing the specific value or values of a parameter.

Modes for filtering events within incidents

When filtering the table of events in tree display mode, incidents that meet the filtering criteria may be presented in the following variants:

- Displayed with all nested elements
- Displayed only with the nested elements that also meet the defined filtering criteria

You can select the relevant display option for incidents by using the **Show embedded events when filtering** check box when configuring the table.

Table search

In a table of a section of the application web interface, you can find relevant items by using the **Search <type of displayed items>** field. The field is displayed in the right part of the section.

A search can be run on selected table columns.

Resetting the defined filter and search settings

In a table of a section of the application web interface, you can reset the defined filter and search settings by clicking **Default filter** in the toolbar. The button is displayed if search or filter settings are defined.

Table sorting

To sort a table:

1. In a table of a section of the application web interface, click the header of the column by which you want to sort.

   The headers of columns that can be sorted are displayed as links.

2. If sorting is performed based on a column that displays different types of values (for example, the **Side 1** column in the **Risks** section), use the drop-down list of the column header to select the settings that will be used for sorting.

3. If you need to sort the table based on multiple columns, press the **SHIFT** key and hold it down while clicking the headers of the columns by which you want to sort.

The table will be sorted by the selected column. When sorting by multiple columns, the rows of the table are sorted according to the sequence of column selection. Next to the headers of columns used for sorting, you will see icons displaying the current sorting order: in ascending order or descending order of values.

Selecting elements in a data table

In a table of a section of the application web interface, you can select any displayed items to view their details and to manage these items. When you select an item in the table, you will see the details area in the right part of the web interface window.

To select the relevant items in the table, do one of the following:

- If you want to select one item, select the check box on the left side of the row containing this item or use your mouse to select the table row.

- If you want to select multiple items, select the check boxes on the left side of the rows containing the relevant items, or select them while holding down **CTRL** or **SHIFT**.

- If you want to select all items that satisfy the current filter and search settings, do one of the following:

  - Select any item in the table and press the key combination **CTRL+A**.

  - Select the check box in the title of the left-most column of the table.

If multiple items are selected, data on their number is displayed in the upper-right corner of the web interface page. The precise number of selected items is displayed up to a specific limit (for example, up to 2,000 items). If more items are selected, the precise number is not displayed (in the above example, `2,000+` will be displayed). If no items are selected in the table, the total number of items in the data table is displayed in the upper-right corner of the page.

The header of the left-most column of the table shows the item selection check box. Depending on the number of selected items, the check box can have one of the following states:

- ☐ – all items that satisfy the current filter and search settings were not selected in the table. In this case, one item or multiple items may be selected in the table by using the check boxes on the left side of rows or by using **CTRL** or **SHIFT**.
- ☑ – all items that satisfy the current filter and search settings are selected in the table.
- ▣ – all items that satisfy the current filter and search settings were selected in the table, but then the check boxes for some of the items were cleared. This state is also retained if the check boxes were cleared for all items selected in this way (due to the fact that the number of selected items may change).

If all items that satisfy the filter and search settings are selected, the number of selected items may automatically change. For example, this could occur as a result of the user's actions in another connection session or when new items are discovered. You are advised to configure the filter and search settings so that you only see the relevant items in the selection.

Navigating to related items in other web interface sections

Items in certain sections of the application web interface (in particular, in data tables) can be associated with the items in other sections containing tables or data structures. For example, events may be related to devices or to risks. When working with such items, you can navigate to the related items in other sections to view details.

To view information about related items:

1. Select the items for which you want to view information about the related items.

   It is recommended to select a limited number of items (up to 200). When you select a large number of items, you may not be able to navigate to view the related items.

2. Open the **Show related** drop-down list in the toolbar.

3. In the drop-down list, select the desired item type (for example, **Devices**).

   A section opens that contains the items of the selected type (in this example, the table of devices in the **Assets** section). The corresponding filtering is applied to display related items.

Exporting data from a table to a file

The data tables of certain sections of the application web interface provide the capability to export data to files in the following formats:

- CSV

  When exporting to this format, the file saves information from the columns currently displayed in the table. Certain data that is not displayed in the table (for example, additional fields and Process Control settings in device information) may also be stored in this format.

- JSON

  When exporting a file in this format, all the data for table items is saved, including service information from the database (such as information about events associated with the devices).

You can export information for all items that satisfy the current filter and search settings, or selectively for items displayed in the table.

To export data for all items that satisfy the current filter and search settings:

1. Click **Export** in the toolbar above the data table to open the menu and select the item with the desired file format: CSV or JSON.

2. If the option to save supplementary settings is available for export, in the window that appears, select the check boxes for the settings that you want to export.

   The file creation process starts.

3. If file generation takes a long time (more than 15 seconds), the operation is moved to the background. If this is the case, follow these steps to download the file:

   a. Click in the application web interface menu.

      The list of background operations opens.

   b. Wait for the file generation operation to complete.

   c. Click **Download file**.

Your browser will save the downloaded file. Depending on your browser settings, your screen may show a window in which you can change the path and name of the saved file.

To export data for the selected items:

1. Select the items whose information you want to export to a file.

2. Right-click to display the context menu of one of the selected items.

3. In the context menu, select the relevant file format option: CSV or JSON.

4. If the option to save supplementary settings is available for export, in the window that appears, select the check boxes for the settings that you want to export.

   The file creation process starts.

5. If it takes a long time (more than 15 seconds) to create the file, perform the necessary actions for step 3 as described in the procedure for exporting data for all items.

Updating a data table

The specific data displayed in a table of a section of the application web interface could possibly be changed on the Server while you are viewing the table (for example, when new items are registered or if data has been modified in a different session of connecting to the Server). Some tables support automatic data updates.

To enable or disable automatic update of data in a table:

In the toolbar above the data table, use the **Update** toggle switch.

Changing your account password

After connecting to the Server through the web interface, you can change the password of your user account that you used to establish the connection. Only a user account that was created in the application can change a user password on the Kaspersky Industrial CyberSecurity for Networks web interface page. This password change method is not available for Kaspersky Security Center user accounts that are configured for Single Sign-On (SSO).

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

- The user has connected for the first time since the account was created or unlocked, or the password was changed by an administrator.

  If the administrator has enabled a mandatory password change for your account the first time you connect to the application after the account has been created and/or after the administrator has changed the password, the **New password** and **Repeat new password** fields will be displayed on the account credentials entry page to change the password.

- The current password has been compromised.

- The password is about to expire.

To change the password of your own user account:

1. On the Kaspersky Industrial CyberSecurity for Networks web interface page, open the user menu:

   - If the menu is collapsed, click the button.

   - If the menu is expanded, click the button on the right of the name of the current user.

2. In the user menu, select **Change password**.

   The **Change password** window appears.

3. In the **Current password** field, enter your current password.

4. Enter the new password in the **New password** and **Repeat new password** fields.

   The new password must meet the conditions listed in the **Change password**. The conditions you fulfill are automatically marked while you are entering your password.

5. Click **Edit**. This button is available after entering the current password and new password and after fulfilling all requirements for the new password.

The new password will be required the next time you connect to the Server through the web interface.

Managing the application through Kaspersky Security Center

The centralized management capabilities of Kaspersky Security Center let you expand the management functionality of Kaspersky Industrial CyberSecurity for Networks and make the application more convenient to use. In addition, Kaspersky Security Center provides centralized management capabilities through the use of policies for other components of the Kaspersky Industrial CyberSecurity solution, such as Kaspersky Industrial CyberSecurity for Nodes and Kaspersky Industrial CyberSecurity for Linux Nodes. Under the management of Kaspersky Security Center, EPP applications scan devices for indicators of compromise. If they are detected, the results are sent to Kaspersky Industrial CyberSecurity for Networks.

The Kaspersky Security Center Administration Server can serve as the source of installed updates for the application. In this case, you will not have to download, copy, and install updates manually or provide Internet access for the Server computer.

This section contains information about configuring interaction between the application and Kaspersky Security Center, and information about using Kaspersky Security Center functions for working with Kaspersky Industrial CyberSecurity for Networks. You can use Kaspersky Security Center to do the following:

- Add a license key to Kaspersky Industrial CyberSecurity for Networks.
- Download updates for application modules and databases to Kaspersky Industrial CyberSecurity for Networks.
- View Kaspersky Industrial CyberSecurity for Networks events in the Kaspersky Security Center Administration Console.
- Monitor the ICS security state in the Administration Console or in a SCADA system.
- Remotely connect to the Kaspersky Industrial CyberSecurity for Networks Server computer.
- Use advanced capabilities of centralized system monitoring with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console.
- Use Single Sign-On technology for authentication of Kaspersky Security Center Web Console users when they connect to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface.

The contents of the available actions list depends on the capabilities of the Kaspersky Security Center version at hand. You can view information about the key features of various Kaspersky Security Center versions in the Kaspersky Security Center Help System.

To enable interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center, the following conditions must be fulfilled:

- The functionality for application interaction with Kaspersky Security Center is added during centralized or local installation of the Kaspersky Industrial CyberSecurity for Networks Server.
- In Kaspersky Industrial CyberSecurity for Networks, the functionality for interaction with Kaspersky Security Center has been enabled and configured.

- The Kaspersky Industrial CyberSecurity for Networks administration plug-in is installed in Kaspersky Security Center (one or two plug-ins depending on the version of Kaspersky Security Center and on the actions that you want to perform using 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** or its subgroup). You can move the device to the administration group when working in the MMC-based Administration Console or when registering Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console.

- Certain ports and protocols used for connections and interactions between the Kaspersky Industrial CyberSecurity for Networks Server and the Kaspersky Security Kaspersky Security Center Administration Server or the Kaspersky Security Center Web Console are available.

Enabling and configuring interaction with Kaspersky Security Center

After the functionality for interaction with Kaspersky Security Center is added to the application during centralized or local installation, this functionality is disabled by default.

To enable and configure the functionality for application interaction with Kaspersky Security Center:

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

2. Select **Settings** → **Kaspersky Security Center**.

3. Use the **Enabled** toggle switch to enable interaction with Kaspersky Security Center.

4. In the **Connector settings** block, configure **Kaspersky Security Center Connector**:

   - IP address / network name of the computer hosting the Kaspersky Security Center Administration Server.

   - SSL port for the connection.

   - Maximum number of relayed events per day, starting at 0:00 in the time zone of the Kaspersky Industrial CyberSecurity for Networks Server. The default value is 2000. You can change the value of this parameter depending on the architecture and size of your system and the specific capabilities of the equipment. Range of entered values: 0–65535.

5. In the **Web plug-in settings for Kaspersky Security Center Web Console** block, configure the settings for connections from the Kaspersky Security Center Web Console:

   - Kaspersky Industrial CyberSecurity for Networks user name that will be indicated in audit log entries when actions are registered from the Kaspersky Security Center Web Console.

   - IP address/network name of the web server on the Kaspersky Industrial CyberSecurity for Networks Server computer.

   - IP address/network name of the REST API server on the Kaspersky Industrial CyberSecurity for Networks Server computer.

6. Click **Apply**.

7. After saving the settings, verify that the conditions have been fulfilled and complete additional configuration for monitoring events via Kaspersky Security Center.

8. Check the connection between Network Agent and the Kaspersky Security Center Administration Server. To do so, on the computer that performs Kaspersky Industrial CyberSecurity for Networks Server functions, open the operating system console and enter the following command:

   ```
   sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

   The screen will display information about the connection to the Administration Server. If the steps are completed successfully, the following messages are displayed on the screen:

   ```
   Connecting to server...OK
   Connecting to the Administration Agent...OK
   ```

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

You can add a license key to Kaspersky Industrial CyberSecurity for Networks by using the functionality for automatic distribution of license keys to Kaspersky Security Center. A license key received in this way is processed in Kaspersky Industrial CyberSecurity for Networks the same as a license key that is added manually in the application.

Automatic license key distribution works if all conditions for communication between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center are met.

To distribute a license key, you need to first add it to the Kaspersky Security Center Administration Server repository. You can add the license key to the storage when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console. To add, use a license key file.

After adding the license key to the Administration Server repository, you can create a license key distribution task when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console.

Receiving updates from the Kaspersky Security Center Administration Server

You can use the Kaspersky Security Center Administration Server as the source of updates for databases and application modules of Kaspersky Industrial CyberSecurity for Networks. This method of receiving updates may be required if, for example, you need to download updates from Kaspersky servers when the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server has no Internet access.

The scenario for preparing the Kaspersky Security Center Administration Server for use as an update source consists of the following steps:

1. **Creating a task in Kaspersky Security Center to download updates to the Administration Server repository**

   You can create a task when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console.

2. **Selecting the Administration Server as an update source in Kaspersky Industrial CyberSecurity for Networks**

   When connected to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface, you can select the Kaspersky Security Center Administration Server as the update source when starting the update process manually and/or when configuring automatic updates.

Monitoring events via Kaspersky Security Center

In Kaspersky Security Center, information about events of Kaspersky Industrial CyberSecurity for Networks is displayed in the following columns of the table of events:

- **Time** or **Event occurred** means the Kaspersky Industrial CyberSecurity for Networks event registration time in the time zone of the computer where Kaspersky Security Center is installed.
- **Device** means the name of the managed device in Kaspersky Security Center (the computer on which Kaspersky Industrial CyberSecurity for Networks Server is installed).
- **Event** means the name of the Kaspersky Security Center event type defined for events of Kaspersky Industrial CyberSecurity for Networks.
- **Description** means the title and brief description of the Kaspersky Industrial CyberSecurity for Networks event.
- **Group** or **Administration group** is the name of the administration group that contains the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server in the **Managed devices** folder in the Kaspersky Security Center Administration Console tree.
- **Application** means the application name (Kaspersky Industrial CyberSecurity for Networks).
- **Version number** means the application version number.
- **Importance level** or **Severity level** means the importance level of the event based on how importance is typified by Kaspersky Security Center.
- **Registered** or **Event registered** means the time at which the event was registered in the Kaspersky Security Center database.

The parameter values of events relayed from Kaspersky Industrial CyberSecurity for Networks are displayed according to the localization settings of Kaspersky Industrial CyberSecurity for Networks. The localization language of Kaspersky Security Center is disregarded for these parameters.

If a Kaspersky Industrial CyberSecurity for Networks event contains information about multiple network interactions, this event is converted into separate items of the Kaspersky Security Center table of events. 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 table of events:

1. Make sure that the required components are installed in Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center.

2. Make sure that the port used for connecting to the computer hosting Kaspersky Security Center is open and accessible on the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server.

3. When configuring the Network Agent policy settings in Kaspersky Security Center, enable saving of relevant events to the Administration Server database and define the event retention period.

   You can configure event registration and retention in the Network Agent policy settings when working in the MMC-based Administration Console or when working in Kaspersky Security Center Web Console.

4. In Kaspersky Industrial CyberSecurity for Networks, configure forwarding of events through the **Kaspersky Security Center Connector**.

When the specific event types are registered in Kaspersky Industrial CyberSecurity for Networks, these events will also be displayed in the Kaspersky Security Center table of events.

Event types in Kaspersky Security Center for Kaspersky Industrial CyberSecurity for Networks events

A fixed set of event types are used for receiving events of Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center. The event types in Kaspersky Security Center correspond to the specific event types in Kaspersky Industrial CyberSecurity for Networks and can be registered as Kaspersky Security Center incidents depending on the severities of the events (see the figure below).

Event types in Kaspersky Security Center for receiving events of Kaspersky Industrial CyberSecurity for Networks

Displayed name of the event type	Code of the event type in Kaspersky Security Center	Registration as a Kaspersky Security Center incident	Corresponding event type code in Kaspersky Industrial CyberSecurity for Networks
Maximum number of reported events reached	32769	yes, with the *Warning* severity level	–
Test event (DPI)	32770	no	4000000001
Test event (NIC)	32771	no	4000000002
Test event (IDS)	32772	no	4000000003
Test event (AM)	32773	no	4000000004
Unauthorized network interaction detected	32774	no	4000002601
System command detected	32775	Only events with a *Critical* severity level	4000002602
No traffic at monitoring point	32776	no	4000002700
TCP protocol anomaly detected: content substitution in overlapping TCP segments	32777	no	4000002701
Process Control rule violation	32778	Only events with a *Critical* severity level	4000002900
Intrusion Detection rule from the system set of rules triggered	32779	no	4000003000
Intrusion Detection rule from the user-defined rule set triggered	32780	no	4000003001

Displayed name of the event type	Code of the event type in Kaspersky Security Center	Registration as a Kaspersky Security Center incident	Corresponding event type code in Kaspersky Industrial CyberSecurity for Networks
Symptoms of ARP spoofing detected in ARP replies	32781	yes	4000004001
Symptoms of ARP spoofing detected in ARP requests	32782	yes	4000004002
New device detected on network	32783	yes	4000005003
New device settings detected	32784	no	4000005004
IP address conflict detected	32785	yes	4000005005
Activity detected from device with Archived status	32786	no	4000005006
New device IP address detected	32787	yes	4000005007
New device MAC address detected	32788	yes	4000005010
MAC address added to the device	32789	no	4000005008
IP address added to the device	32790	no	4000005009
PLC Project Control: detected reading of unknown block from PLC	32791	no	4000005200
PLC Project Control: detected reading of known block from PLC	32792	no	4000005201
PLC Project Control: detected writing of new block to PLC	32793	no	4000005202
PLC Project Control: detected writing of known block to PLC	32794	no	4000005203
PLC Project Control: detected reading of unknown project from PLC	32795	no	4000005204
PLC Project Control: detected reading of known project from PLC	32796	no	4000005205
PLC Project Control: detected writing of new project to PLC	32797	no	4000005206
PLC Project Control: detected writing of known project to PLC	32798	no	4000005207
IP protocol anomaly detected: data conflict when assembling IP packet	32799	no	4000005100
IP protocol anomaly detected: fragmented IP packet size exceeded	32800	no	4000005101
IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	32801	no	4000005102
IP protocol anomaly detected: mis-associated fragments	32802	no	4000005103
Correlation rule event registered	32803	Only events with a *Critical* severity level	8000000001
Event from external system	32804	Only events with a *Critical* severity level	4000005400
Different MAC address for a device is found in data received from EPP application	32805	yes	4000005011
New address information for a device is found in data received from EPP application	32806	yes	4000005012
Conflict detected in device addresses after receiving data from EPP application	32807	yes	4000005013

Displayed name of the event type	Code of the event type in Kaspersky Security Center	Registration as a Kaspersky Security Center incident	Corresponding event type code in Kaspersky Industrial CyberSecurity for Networks
Subnet added based on data from EPP application	32808	yes	4000005014
Device equipment change detected	32809	no	4000005015

Correspondence of Kaspersky Security Center event severity levels

The severities of events in Kaspersky Security Center correspond to the severity levels of events in Kaspersky Industrial CyberSecurity for Networks (see the table below). For the severity levels of Kaspersky Industrial CyberSecurity for Networks events, the corresponding names of severity levels used in previous application versions are specified.

Correspondence between event severities

Kaspersky Security Center event severities	Kaspersky Industrial CyberSecurity for Networks event severities
Info	*Low* (*Informational*)
Warning	*Medium* (*Warning*)
Critical	*High* (*Critical*)

Monitoring the ICS security state: Kaspersky Security Center and SCADA

Kaspersky Industrial CyberSecurity for Networks can relay data about the ICS security state to Kaspersky Security Center. To transmit data to Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center, the required components must be installed.

If the transmission of ICS security state data to Kaspersky Security Center has been configured, you can configure the SCADA system to receive the corresponding information from Kaspersky Security Center.

To configure a SCADA system to receive and display the ICS security state:

1. Install Kaspersky Security Gateway on the computer hosting Kaspersky Security Center.

   You can find detailed information on installing and configuring Kaspersky Security Gateway in the *Kaspersky Security Gateway Administrator Guide*.

2. In the SCADA system, create a control element that reflects the state of the computer with Kaspersky Industrial CyberSecurity for Networks.

3. Configure the created control element to receive data over the OPC DA 2.0 or IEC 60870-5-104 protocol.

   Instructions on configuring the control element are provided in the *Kaspersky Security Gateway Administrator Guide*.

Connecting to the Server computer from Kaspersky Security Center

You can remotely connect to the Kaspersky Industrial CyberSecurity for Networks Server computer from the Kaspersky Security Center Administration Console. This requires the use of the MMC-based Administration Console. The Virtual Network Computing (VNC) remote desktop access system is used to make the connection.

To connect, you must install and configure the following VNC components:

- VNC server. It is installed on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server. When configuring the VNC server, you need to set a password for the VNC connection. If a firewall is enabled on the computer, you also need to open the ports for the VNC and SSH protocols.
- VNC client. It is installed on the computer that has the Kaspersky Security Center Administration Console.

To gain access to the Kaspersky Industrial CyberSecurity for Networks Server computer from Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the computer on which the Kaspersky Industrial CyberSecurity for Networks Server is installed.
3. In the workspace on the **Devices** tab, select the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server, and select **Custom 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 **Custom tools** → **Configure custom tools**. In the **Custom 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 **Work folder** field, enter the full path to the working folder of the VNC client (for example, `C:\Program Files\TightVNC\`).
   - In the **Command line** field, enter the following value: `<A>:<P>`.
   - Select the **Create tunnel for TCP port specified below** check box and enter the number of the VNC port on the VNC server (for example, if the VNC server uses screen :3, enter the VNC port number `5903`).
4. After the external VNC tool is started, a password prompt window appears. Enter the password for the VNC connection.

The opened window displays the desktop of the computer on which the Kaspersky Industrial CyberSecurity for Networks Server is installed.

Centrally monitoring systems with Kaspersky Industrial CyberSecurity for Networks from the Kaspersky Security Center Web Console

The Kaspersky Security Center Web Console (hereinafter also referred to as "the Web Console") provides expanded capabilities for centrally monitoring the security state of information systems running Kaspersky Industrial CyberSecurity for Networks. These expanded capabilities are available when using the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in (hereinafter also referred to as "the web plug-in") in the Web Console. To use the web plug-in, it must be installed on the computer that has the Kaspersky Security Center Web Console installed.

After installing and configuring the web plug-in, you can do the following in the Web Console:

- Monitor systems controlled by Kaspersky Industrial CyberSecurity for Networks and the Kaspersky Industrial CyberSecurity for Networks Servers by using widgets designed only for working with Kaspersky Industrial CyberSecurity for Networks.
- Search devices and events in the databases of selected Kaspersky Industrial CyberSecurity for Networks Servers using various filtering criteria.
- Map components and groups of components of Kaspersky Industrial CyberSecurity for Networks on geographic, schematic or other images to arrange objects based on their location.
- Group components of Kaspersky Industrial CyberSecurity for Networks into organizational units (hereinafter also referred to as "sites") that logically delimit the areas of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks.

When using the functions listed above, you can quickly switch from the Web Console to connect to the necessary Kaspersky Industrial CyberSecurity for Networks Servers through the web interface. If Single Sign-On technology is in use, users who were created in Kaspersky Industrial CyberSecurity for Networks do not have to enter their account credentials when connecting to a Kaspersky Industrial CyberSecurity for Networks Server. Users who have logged in to the Web Console can also complete authentication.

About updating the Kaspersky Industrial CyberSecurity for Networks administration web plug-in

The installed Kaspersky Industrial CyberSecurity for Networks administration web plug-in facilitates interaction between the application and the Kaspersky Security Center Web Console.

You can view the list of installed web plug-ins in the Web Console interface: **Console settings** → **Web plug-ins**.

If a new version of the web plug-in becomes available, the Web Console displays the *Updates are available for utilized plug-ins* notification. You can proceed to update the web plug-in version from this Web Console notification. You can also manually check for new web plug-in updates in the Web Console interface (**Console settings** → **Web plug-ins**). The previous version of the web plug-in will be automatically removed during the update.

When the web plug-in is updated, existing components (such as the added widgets or map images) are saved. The new settings of components that implement new functions of Kaspersky Industrial CyberSecurity for Networks will have the default values.

You can update the web plug-in by using any of the following methods:

- Update the web plug-in in the list of web plug-ins in online mode.

  To update the web plug-in, select the distribution package of the Kaspersky Industrial CyberSecurity for Networks web plug-in in the Web Console interface and start the update (**Console settings** → **Web plug-ins**). The Web Console checks for available updates on Kaspersky servers and downloads the relevant updates.

- Update the web plug-in from a file.

  To update the web plug-in, select the ZIP-archive of the distribution package for the Kaspersky Industrial CyberSecurity for Networks web plug-in in the Web Console interface: **Console settings** → **Web plug-ins**. The distribution package of the web plug-in can be downloaded from the Kaspersky website, for example. For a local version of the application, you also need to download a text file containing a signature.

  You can only update the web plug-in to a more recent version. The web plug-in cannot be updated to an older version.

Scenario for Single Sign-On (SSO) technology usage preparations

When working in combination with Kaspersky Security Center, you can use Single Sign-On (SSO) technology. This enables users that already logged in to the Kaspersky Security Center Web Console to also successfully complete authentication when connecting to the Kaspersky Industrial CyberSecurity for Networks Server through the web interface. This means that any user accounts that are allowed to work with the Kaspersky Security Center Web Console (including Active Directory® users) can connect to the Server using their own account credentials.

Single Sign-On technology is available for use with Kaspersky Industrial CyberSecurity for Networks in the compatible versions of Kaspersky Security Center:

The Single Sign-On (SSO) technology usage preparations scenario consists of the following steps:

1. **Verifying and fulfilling the required conditions for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center**

   At this step, you need to verify fulfillment of all conditions for interaction between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center. If any of the conditions is not fulfilled, ensure that they get fulfilled. For example, if the functionality for interacting with Kaspersky Security Center is not configured in Kaspersky Industrial CyberSecurity for Networks, enable and configure this functionality.

2. **Enabling and configuring the Kaspersky Security Center Web Console Identity and Access Manager (IAM) component**

   At this step, the scenario for enabling Identity and Access Manager is executed as described in the Kaspersky Security Center Help System.

   When configuring the IAM component, it is recommended to specify the DNS name of the computer as the network name of the device only if the computer is accessible by this name from the Kaspersky Industrial CyberSecurity for Networks Server computer. If it is accessible only by IP address, specify this IP address instead of the DNS name.

3. **Registering the Kaspersky Industrial CyberSecurity for Networks Server as a client for the IAM component**

   At this step, the IAM component detects Kaspersky Industrial CyberSecurity for Networks Servers that are prepared for registration as clients for this component. You need to accept the request for Server registration after it is detected. Detected and registered clients of the IAM component are displayed in a table that you can open in the Kaspersky Security Center Web Console under **Console settings** → **Integration** → **Identity and Access Manager**. To register Servers, open the table by clicking the **Settings** link in the section containing information about registered clients, select the check boxes next to the relevant Servers, and click **Approve**.

   After you have confirmed registration of the IAM component client, you need to wait for the preparation process to finish. When synchronization between the IAM component and the client is completed, the ready status will be displayed for this client. If the status has not changed, click the **Refresh** button.

   > The IAM component needs some time to detect clients and synchronize with them. Depending on the workload of the Kaspersky Security Center Administration Server and the Kaspersky Industrial CyberSecurity for Networks Server, it may take up to 15 minutes to complete these actions.

4. **Preparing users with access permissions for connecting to Kaspersky Industrial CyberSecurity for Networks**

   At this stage, you need to grant access permissions to Kaspersky Security Center users according to their roles in Kaspersky Industrial CyberSecurity for Networks: Administrator, Security Officer, Infrastructure Officer, ICS Officer, and Operator. For this purpose, you can use existing user accounts or new accounts of users and groups that were created specifically for granting only these permissions.

When this scenario is fulfilled, Kaspersky Industrial CyberSecurity for Networks will have the capability to connect to the Server through the web interface using the account credentials of Kaspersky Security Center users. To do so, you can use the **Kaspersky Security Center user** button on the account credentials input page for the Kaspersky Industrial CyberSecurity for Networks web interface. After connecting to the Server, users can perform any actions in the application if they have been granted the appropriate privileges. The application does not ask these users to enter a password to perform operations that require password confirmation (for example, to initiate certain response actions).

> If a fully qualified domain name (FQDN) was specified for the web server and the REST API server when configuring the connection settings using Kaspersky Security Center Web Console, then when connecting to the Kaspersky Industrial CyberSecurity for Networks Server using single sign-on technology, the user must also specify this name in the address bar of the browser.

Granting Kaspersky Security Center users the access rights corresponding to their user roles in Kaspersky Industrial CyberSecurity for Networks

To utilize Single Sign-On technology and perform specific actions in the Web Console, Kaspersky Security Center users must be granted the access permissions corresponding to their user roles in Kaspersky Industrial CyberSecurity for Networks. You can grant these permissions after the file containing the configuration of the rights-based access control model (RBAC) for Kaspersky Industrial CyberSecurity for Networks has been uploaded to the Kaspersky Security Center Administration Server.

The configuration is loaded automatically after installation of the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in. If the configuration was uploaded to the Administration Server, the file named KICS4NET_<file version number>.conf was saved in the folder %ProgramData%\KasperskyLab\adminkit\1093\dat\rbac\. If the specified folder does not contain the file named KICS4NET_<file version number>.conf, create and configure the "Download updates to the Administration Server repository" task. You can select the Kaspersky update servers as the source of updates.

After loading the RBAC configuration for Kaspersky Industrial CyberSecurity for Networks, Kaspersky Security Center provides the ability to assign users the privileges that correspond to the Administrator, Security Officer, Infrastructure Officer, ICS Officer, and Operator roles in Kaspersky Industrial CyberSecurity for Networks.

User roles in Kaspersky Industrial CyberSecurity for Networks have the following corresponding access rights in Kaspersky Security Center from the functional scope of **Kaspersky Industrial CyberSecurity for Networks: General features**:

- **Read**: for the Administrator, Security Officer, Infrastructure Officer, ICS Officer, and Operator roles
- **Write**: for the Administrator, Security Officer, Infrastructure Officer, and ICS Officer roles
- **Execute**: for the Administrator and Security Officer roles
- **Manage certificates**: for the Administrator role
- **Modify object ACLs**: for the Administrator role
- **Edit event logging settings**: for the Administrator and Security Officer roles
- **Edit event notification settings**: for the Administrator role
- **Configure hierarchy of Administration Servers** for the Administrator role
- **Save files from devices to the administrator's workstation**: for the Administrator, Security Officer, and ICS Officer roles
- **Export key file**: for the Administrator role
- **Delete events**: for the Administrator role
- **Perform operations on device selections**: for the Administrator and Security Officer roles

Together with these rights, users must also be assigned all rights from the functional scope of the **Kaspersky Security Center Administration Server: General features: Basic functionality** (this functional scope includes the rights to **Read**, **Write**, **Execute** and **Perform operations on device selections**).

If access rights are assigned to users by means of Kaspersky Security Center roles, then you must add the administration group containing the computer with the Kaspersky Industrial CyberSecurity for Networks Server installed to the role scope. To do so, on the **Define scope** page in the Role Assignment Wizard, select the **Managed Devices** administration group.

Widgets for monitoring systems and Kaspersky Industrial CyberSecurity for Networks Servers

You can use widgets to monitor systems controlled by Kaspersky Industrial CyberSecurity for Networks and Kaspersky Industrial CyberSecurity for Networks Servers. The Kaspersky Security Center Web Console displays widgets in the Dashboard (under **Monitoring & reporting** → **Dashboard**). By default, the Dashboard does not show widgets for Kaspersky Industrial CyberSecurity for Networks. You can add the necessary widgets after installation of the Kaspersky Industrial CyberSecurity for Networks Administration web plug-in.

Widgets let you show the following information in the Dashboard:

- Statuses in KICS for Networks.
- Critical events in KICS for Networks.
- Devices with issues in KICS for Networks.
- Up-to-date events of KICS for Networks.
- KICS for Networks deployment map.
- Information about KICS for Networks Servers.

Widgets for Kaspersky Industrial CyberSecurity for Networks are included in the **Other** category in the list of available widgets of the Web Console.

The information displayed in widgets is automatically updated every 1–2 minutes. If no data is received from a Server after two minutes, out-of-date data in widgets is hidden. If necessary, you can manually update the displayed information by using the relevant options in the widget menu.

Widget for Statuses in KICS for Networks

The **Statuses in KICS for Networks** widget for the Web Console displays the ratio of current statuses assigned to Kaspersky Industrial CyberSecurity for Networks Servers. Information is provided only for relevant statuses (if there are no Servers with a specific status, this status is not displayed in the widget).

The following statuses are available for Servers in the widget:

- *Critical*

This status is assigned to a Server if at least one of the following conditions is fulfilled:

- The Server has messages about disruption of application operation.
- The Server database has unresolved events with *Critical* severity.
- There are devices with a status of *Unauthorized*.
- The license key expired.

- *Warning*

  This status is assigned to a Server if none of the conditions for assigning a status of *Critical* are fulfilled, but at least one of the following conditions is fulfilled:

  - The Server has messages about non-critical malfunctions.
  - The Server database has unresolved events with *Warning* severity.
  - The license key will expire in less than 14 days.

- *OK*

  This status is assigned to a Server in all other cases (if the Server is accessible and data is being received for processing).

- *Maintenance*

  This status is assigned to a Server if the application is currently under maintenance (for example, when importing a security policy).

If the status of a Server cannot be determined, a status of *Unknown* is displayed for this Server.

By default, the widget displays status information for all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the widget. If necessary, you can use the widget settings menu to select the Servers whose data should be displayed in the widget.

Widget for Critical events in KICS for Networks

The **Critical events in KICS for Networks** widget for the Web Console displays the ratio of unresolved events with *High* severity (corresponding to the *Critical* severity level) on Kaspersky Industrial CyberSecurity for Networks Servers. For each Server whose database contains unresolved events with *High* severity (corresponding to the *Critical* severity level), the number of these events is displayed.

The different coloring of data presented in the widget does not have any relation to the severity of events. Colors on the widget chart are used only to visually distinguish events of different Servers.

By default, the widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the widget. If necessary, you can use the widget settings menu to select the Servers whose data should be displayed in the widget.

Widget for Devices with issues in KICS for Networks

The **Devices with issues in KICS for Networks** widget for the Web Console displays information about devices that were detected by Kaspersky Industrial CyberSecurity for Networks applications and have issues. A device requires attention (designated as "with issues") in any of the following cases:

- The security state of the device differs from *OK*.
- The device has a status of *Unauthorized*.

If there are devices with issues, the widget contains the following information:

- Number of devices with issues (in each device category). This data is displayed in the upper part of the widget under the icons of device categories. The number of displayed categories depends on the free space in the widget. If there are more categories to display, you can open a window containing all categories by clicking **Show all**.
- List of categories of devices with issues. This data is displayed in the middle part of the widget. The following information is displayed for each category in the list:
  - Line containing the category icon and comment. The end of the line provides a link containing the number of devices with issues.
  - Line containing the graphical elements representing the devices. This line is displayed if there is sufficient free space in the widget. If there are more devices with issues than the number of graphical elements displayed in the line, the number of hidden devices is displayed on the right in the format `+<number of devices>`.

By default, the widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the widget. If necessary, you can use the widget settings menu to select the Servers whose data should be displayed in the widget.

Graphical elements of devices

Graphical elements representing devices contain the following information:

- Device name.
- Device status. This is displayed as an icon if the device has a status of *Unauthorized*.
- Device security state. This is displayed as a colored line on the left border of the graphical element. The color of the line corresponds to the *OK*, *Warning*, or *Critical* states.

The graphical elements are displayed in the following order:

1. Devices assigned a status of *Unauthorized*.
2. Devices with a *Critical* security state.
3. Devices with a *Warning* security state.

Navigating from the widget

You can use elements of the widget interface to display detailed information about devices. The following options are available to achieve this.

Display information about the selected device in the table of devices on the Server web interface page.

In the **Devices with issues in KICS for Networks** widget, click the graphical element that represents the relevant device.

The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during startup configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

On the Server web interface page, the **Assets** section automatically opens to show the table of devices. The table will be filtered based on the device ID.

Display information about devices of the selected category in the search results table in the Web Console

To display information about all devices of the selected category:

In the upper part of the **Devices with issues in KICS for Networks** widget, click the icon of the relevant category.

The **KICS for Networks → Search** section of the Web Console opens to display a table of device search results. The table will be filtered based on the following criteria:

- Selected category of devices
- All Servers whose data is taken into account in the widget

To display information about all devices with issues that belong to a specific category:

In the list of categories containing devices with issues, click the link containing the number of devices of the relevant category.

The **KICS for Networks → Search** section of the Web Console opens to display a table of device search results. The table will be filtered based on the following criteria:

- Selected category of devices
- All Servers whose data is taken into account in the widget
- Indicator of devices with issues

Display information about all devices in the search results table in the Web Console

Click **Show all devices** in the **Devices with issues in KICS for Networks** for Networks widget.

The **KICS for Networks → Search** section of the Web Console opens to display a table of device search results. The table will be filtered for all Servers whose data is taken into account in the widget.

Widget for Up-to-date events of KICS for Networks

The **Up-to-date events of KICS for Networks** widget for the Web Console displays general information about Kaspersky Industrial CyberSecurity for Networks events that have the most recent values for the date and time of last occurrence.

The widget contains the following information:

- Histogram of events for the selected period. This data is displayed in the upper part of the widget. The histogram shows the distribution of events by severity levels.
- List of registered events. This data is displayed in the middle part of the widget. Events are sorted by date and time of last occurrence.

By default, the widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If data is not received from a Server after two minutes, the out-of-date information is no longer displayed in the widget. If necessary, you can use the widget settings menu to select the Servers whose data should be displayed in the widget.

Histogram of events

On the histogram showing the distribution of events, the bars correspond to the total number of events for each time interval. Within bars, the severity of events is distinguished by color. The following colors correspond to severity levels:

- Blue – events with *Low* severity (corresponding to the *Informational* severity level).
- Yellow – events with *Medium* severity (corresponding to the *Warning* severity level).
- Red – events with *High* severity (corresponding to the *Critical* severity level).

When you move the mouse pointer over a bar of the histogram, a pop-up window showing the number of events by severity levels is displayed.

The duration of time intervals depends on the selected display period. To build the relevant histogram, you can select one of the following periods from the widget menu:

- 1 hour. This period is divided into one-minute intervals.
- 12 hours, 24 hours. These periods are divided into one-hour intervals.
- 7 days. This period is divided into 12-hour intervals.

List of events

The number of displayed elements in the list of events is limited by the size of the widget.

The following information is provided for each event:

- Event title
- Severity level
- Name of the computer hosting the Kaspersky Industrial CyberSecurity for Networks Server

Navigating from the widget

You can use elements of the widget interface to display detailed information about events. The following options are available to achieve this.

Display information about the selected event in the table of events on the Server web interface page.

Click the relevant event in the **Up-to-date events of KICS for Networks** widget.

The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during startup configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

On the Server web interface page, the **Events** section automatically opens to show the table of events. The table will be filtered based on the ID of the selected event. The period ranging from the date and time of registration of the event to the current moment (without indicating an end boundary for the period) will also be defined for the filter.

Display information about all events for the selected period in the search results table in the Web Console.

Click **Show all events** in the **Up-to-date events of KICS for Networks** widget.

The **KICS for Networks** → **Search** section of the Web Console opens to display a table of event search results. The table will be filtered based on the following criteria:

- Currently selected period for building a histogram in the widget
- All Servers whose data is taken into account in the widget

Widget for KICS for Networks deployment map

The **KICS for Networks deployment map** widget for the Web Console displays a map depicting the geographic distribution of sites in which Kaspersky Industrial CyberSecurity for Networks components are grouped. The widget uses a smaller copy of the main map that is available in the **KICS for Networks** → **Map** section of the Web Console.

Sites on the map are designated by icons whose color depends on the statuses of the sites. The following statuses are available for sites:

- *Critical*

  This status is assigned to a site if it contains at least one Server with a status of *Critical*.

- *Warning*

  This status is assigned to a site if it contains at least one Server with a status of *Warning* and does not contain Servers with a status of *Critical* or *Unknown*.

- *OK*

  This status is assigned to a site if it contains at least one Server with a status of *OK* and does not contain Servers with a status of *Critical*, *Warning*, *Unknown*, or *Maintenance*.

- *Maintenance*

  This status is assigned to a site if it contains at least one Server with a status of *Maintenance* and does not contain Servers with a status of *Critical*, *Warning*, or *Unknown*.

- *Muted*

  This status is assigned to a site if it contains only Servers with a status of *Muted*.

- *Unknown*

  This status is assigned to a site if it contains at least one Server with a status of *Unknown* and does not contain Servers with a status of *Critical*.

- *No Servers*

  This status is assigned to a site if it does not contain any Servers.

You can proceed to the main map in the **KICS for Networks** → **Map** section of the Web Console by clicking any part of the map except the icons of sites.

You can proceed to a site map by clicking the icon of this site in the widget.

Widget for Information about KICS for Networks Servers

The **Information about KICS for Networks Servers** widget for the Web Console displays general information about the current state of Kaspersky Industrial CyberSecurity for Networks Servers.

The following information is provided for each Server:

- **Server name** – name used to represent the Server in Kaspersky Security Center (device name in the administration group).
- **Functions** – information about the current state of protection functions in Kaspersky Industrial CyberSecurity for Networks. The following values are possible:
  - **All ON** – all technologies and methods designed for continual use are enabled, and all created monitoring points are enabled.
  - **Not all ON** – some protection functions are disabled or are enabled in learning mode, or not all monitoring points are enabled.
- **Status** – current status of the Server.
- **Application message** – last application message or additional status information.

By default, the widget displays information based on the data received by the Web Console from all Servers in Kaspersky Security Center administration groups. If necessary, you can use the widget settings menu to select the Servers whose data should be displayed in the widget.

You can click the link containing a Server name to open the web interface page of the selected Kaspersky Industrial CyberSecurity for Networks Server. The name of the opened browser tab will be the Server name that was defined during startup configuration of the application after installation.

If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

Searching devices and events in the databases of Kaspersky Industrial CyberSecurity for Networks Servers

In the Kaspersky Security Center Web Console, you can create requests to receive specific selections of devices and events by using the Kaspersky Industrial CyberSecurity for Networks web plug-in. Based on these requests, a search is performed directly in the databases of Kaspersky Industrial CyberSecurity for Networks Servers. This is the main distinction between the web plug-in capabilities and the search functionality provided by the standard tools for receiving selections of devices and events in the Web Console (for example, under **Devices → Device selections** and **Monitoring & reporting → Event selections**). When using the standard tools in the Web Console, the search for devices and events is performed in the Administration Server database.

The **KICS for Networks → Search** section of the Web Console is used to configure the settings of search requests sent to Kaspersky Industrial CyberSecurity for Networks Servers and to display the search results. Search requests for devices must be formulated separately from search requests for events.

Kaspersky Industrial CyberSecurity for Networks Servers process the search requests and provide information for those requests with the following limitations:

- The number of returned items that match the search request (devices or events) from each Server cannot be more than 200.
- They provide only the information that can actually be searched. For example, device search results will contain the MAC- and IP addresses of devices but will not contain information about the device models and manufacturers.

In any case, when you need to obtain complete information about any found devices or events, you can go to the web interface page of the Server by using the interface elements under **KICS for Networks → Search**. The Server web interface page automatically opens the corresponding section (**Assets** or **Events**), which will be filtered based on the criteria of the search request or the obtained results.

Configuring the device search settings

You can manually configure the device search settings or use automatically applied filtering criteria when navigating directly from the **Devices with issues in KICS for Networks** widget.

To manually configure these settings, you need to open the **Devices** tab in the search request details area.

*To open the **Devices** tab in the search request details area:*

1. Go to the **KICS for Networks** → **Search** section of the Web Console.
2. Do one of the following:
   - If a search request was not created during the current session and this section is not displaying a search results table, click **Find events or devices**.
   - If a search request was created in the current session and this section is displaying a search results table, click **Search** in the toolbar.

     The **Search** button displays the number of filtering criteria (defined settings) of the current search request.
3. In the search request details area, go to the **Devices** tab.

After configuring the settings, you can start searching for devices in the databases of Servers by clicking **Find**.

You can configure the following settings in a device search request:

- **Name** – name that represents the device in the table of devices of the Kaspersky Industrial CyberSecurity for Networks Server. The complete name must be specified.
- **Servers** – names that represent the Servers in Kaspersky Security Center (device names in administration groups).
- **Addresses** – device MAC and/or IP addresses. Complete addresses must be provided.
- **Statuses** – device statuses that determine whether activity of the devices is allowed in the industrial network.
- **Security states** – device security states that are determined by the severity of registered events linked to the device and current vulnerabilities.
- **Categories** – names of the categories that determine the functional purpose of devices.
- **With issues** – indicates whether the device has issues requiring attention.

You can clear the defined settings in a search request by clicking **Reset filters**.

Configuring the event search settings

You can manually configure the event search settings or use automatically applied filtering criteria when navigating directly from the **Up-to-date events of KICS for Networks** widget.

To manually configure these settings, you need to open the **Events** tab in the search request details area.

*To open the **Events** tab in the search request details area:*

1. Go to the **KICS for Networks** → **Search** section of the Web Console.
2. Do one of the following:
   - If a search request was not created during the current session and this section is not displaying a search results table, click **Find events or devices**.
   - If a search request was created in the current session and this section is displaying a search results table, click **Search** in the toolbar.

     The **Search** button displays the number of filtering criteria (defined settings) of the current search request.
3. In the search request details area, go to the **Events** tab.

After configuring the settings, you can start searching for events in the databases of Servers by clicking **Find**.

You can configure the following settings in an event search request:

- **Title** – title defined for the event type in Kaspersky Industrial CyberSecurity for Networks. The complete title must be specified.
- **Servers** – names that represent the Servers in Kaspersky Security Center (device names in administration groups).
- **Last seen** – period for filtering events by date and time of last appearance.
- **Source** – address information (MAC/IP addresses or port numbers) of the senders of network packets.
- **Destination** – address information (MAC/IP addresses or port numbers) of the recipients of network packets.
- **Technologies** – icons and names of technologies that were used to register the events.
- **Severity** – icons and names of the event severity levels.

You can clear the defined settings in a search request by clicking **Reset filters**.

Viewing the search results table

The search results table for devices or events is displayed in the **KICS for Networks** → **Search** section of the Web Console. The table shows only the data that can be used to perform a device search or event search. Any found items are grouped based on their respective Servers.

When viewing the table, you can utilize the following functions:

- Filtering search results.

  To filter the search results table, you can utilize the following interface elements in the toolbar:

  - **Security states**

    This filter is available in the results table for device searches. You can use the filter buttons to hide some of the found devices depending on their security states.

- **Severity**

  This filter is available in the results table for event searches. You can use the filter buttons to hide some of the found events depending on their severity levels.

- **Technologies**

  This filter is available in the results table for event searches. You can use the filter buttons to hide some of the found events depending on the technologies that were used to register them.

- **Servers**

  This drop-down list lets you select specific Servers for displaying search results.

- Updating search results.

  Information about devices or events could be changed on the Servers while you are viewing the search results table. The **Last updated** field displays the date and time when the results were last loaded.

  You can repeat a search request to update the results by clicking **Update** in the toolbar.

- Displaying information on Server web interface pages.

  Do one of the following:

  - To receive detailed information about one of the found items, open the web interface page of the corresponding Server by clicking the link containing the device name or the event title.

  - To receive information about all the found items that meet the search request criteria, open the web interface page of the corresponding Server by clicking **Go to Server**.

  The Kaspersky Industrial CyberSecurity for Networks Server web interface page opens on a new tab in the browser window. The name of the opened tab will be the Server name that was defined during startup configuration of the application after installation.

  If Single Sign-On technology is in use and the Web Console user has the permissions to connect to this Server, access to the Server web interface will be granted without prompting the user for their user account credentials.

  On the Server web interface page, the relevant section automatically opens to show the table of devices or table of events. The table will be filtered based on the corresponding criteria.

Mapping components of Kaspersky Industrial CyberSecurity for Networks

The web plug-in lets you create maps depicting the deployment of Servers and sensors of Kaspersky Industrial CyberSecurity for Networks in the Kaspersky Security Center Web Console. You can use maps to arrange these items based on their geographic location and to monitor their state in a view that is convenient for you.

The **KICS for Networks** → **Map** section of the Web Console is designed for working with maps. This section displays the following maps (only one map can be selected at one time):

- Main map. This map depicts the various sites (organizational units used to group components of Kaspersky Industrial CyberSecurity for Networks). Servers and sensors are not displayed at this level.

- Site maps. Each site map contains the application components (Servers and sensors) that are included in this particular site.

On maps, sites and application components are represented by icons containing the names of these objects. Long names are abbreviated to their first characters.

Background images can be displayed in various scales. To manage the display scale, you can use the toolbar located in the upper part of the **KICS for Networks** → **Map** section of the Web Console.

After navigating from the main map to a site map, you can return to the main map by using the arrow button.

Only Kaspersky Security Center users who have been granted the access permissions for the Administrator role in Kaspersky Industrial CyberSecurity for Networks can create maps and arrange objects on those maps. When configuration is complete, users with access permissions for the Operator role can track the state of objects by using the maps in the Web Console under **KICS for Networks** → **Map** and in the **KICS for Networks deployment map** widget.

Generating a list of sites for the main map

This section describes the features for generating a list of sites for the main map.

When working with the main map in the **KICS for Networks** → **Map** of the Web Console, you can generate a list of sites that will be used to delimit the zones of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks. You can add relevant Servers and perform operations with these Servers and their sensors within sites.

The maximum number of sites is 100.

A list of sites can be generated only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

Adding a site

To add a site for the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. Click **Add**.

   A window for entering the site name appears.
5. Enter the site name.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

The site name must meet the following requirements:

- Must begin and end with any permitted character except a space.
- Must contain 255 characters or less.
- Must not match the name of another site.

The **Sites** window will show a line containing the name of the new site.

6. If a line containing the site name has not appeared in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking **All statuses** or enable the display of sites without Servers by clicking **No Servers**.
7. Add the site to the main map. To do so, move your cursor over the line containing the site name and click the button.
8. Move the site icon to the necessary place on the map.

Renaming a site

To rename a site for the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking **All statuses** or click the name of the status that was assigned to the relevant site.
5. Move your cursor over the line containing the site name and click the button.

   A window for entering the site name appears.
6. Enter the site name.

   You can use letters, numerals, a space, and the following special characters: `! @ # № $ % ^ & ( ) [ ] { } ' , . - _`.

   The site name must meet the following requirements:

   - Must begin and end with any permitted character except a space.
   - Must contain 255 characters or less.
   - Must not match the name of another site.

Deleting a site

To remove a site for the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking **All statuses** or click the name of the status that was assigned to the relevant site.
5. Move your cursor over the line containing the site name and click the × button.
6. In the confirmation prompt window, click **OK**.

Changing the background image of a map

After a map is created, the map uses the default background image. You can change the background image to any image you want. For example, you can use the image of a geographic map of any territory for the main map, and you can upload equipment deployment schematics of workshops and work areas for site maps.

For a map background, you can use images uploaded from JPG or PNG files. The maximum size of an uploaded file is 50 MB. The minimum size of an image in an uploaded file is 600x600 pixels. After a new image is uploaded, the old image is deleted and the positions of all objects on the map are cleared.

The background image on maps can be changed only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

To change the background image for the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Replace image**.

   You will see a window prompting you to drag the image file or select a file.
4. Use any convenient method to upload the file.

To change the background image for a site map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.

3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click **Replace image**.

   You will see a window prompting you to drag the image file or select a file.

6. Use any convenient method to upload the file.

Generating lists of Servers within sites

This section describes the features available for generating lists of Servers within sites.

On the maps of created sites under **KICS for Networks** → **Map** in the Web Console, you need to generate lists of Servers residing at these sites based on the delimited zones of control and/or deployment of Kaspersky Industrial CyberSecurity for Networks. Any Servers residing at sites also include the sensors that are associated with these Servers.

Each Kaspersky Industrial CyberSecurity for Networks Server can be included in only one site. Any Server that was not added to a site will remain on the **Outside of sites** list until it is included in a site.

Lists of Servers at sites can be generated only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

Adding a Server to a site

To add a Server to a site:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click **Show list of Servers**.

   A window containing the site name will appear in the right part of the section.

6. Select the **Outside of sites** tab.

7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking **All statuses** or click the name of the status that was assigned to the relevant Server.

8. Move your cursor over the line containing the Server name and click the + button.

   The Server line will no longer be displayed on the **Outside of sites** tab.

9. Select the **In site** tab.

10. If a line containing an added Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking **All statuses** or click the name of the status that was assigned to the Server.

11. Add the Server to the site map. To do so, move your cursor over the line containing the Server name and click the button.

    After this operation is performed, the brightness of the icon in the button changes.

12. If there are sensors associated with the Server and you want to enable the display of these sensors, expand the **Sensors** and add them by using the buttons.

13. Move the icons of objects to their proper positions on the map.

Removing a Server from a site

To remove a Server from a site:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.

2. Select **KICS for Networks** → **Map**.

3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.

4. Click the line containing the name of the relevant site.

   The site map opens.

5. Click **Show list of Servers**.

   A window containing the site name will appear in the right part of the section.

6. Select the **In site** tab.

7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking **All statuses** or click the name of the status that was assigned to the relevant Server.

8. Move your cursor over the line containing the Server name and click the × button.

   The Server will appear on the **Outside of sites** tab.

Managing the arrangement of objects on maps

In the **KICS for Networks** → **Map** section of the Web Console, sites and components of Kaspersky Industrial CyberSecurity for Networks are represented by icons on maps.

The arrangement of objects on maps can be managed only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

You can move the icons of objects to their necessary locations on maps. However, all icons on a map must be displayed separately without completely overlaying each other.

If necessary, you can disable the display of an irrelevant object on a map. After being disabled from the display, an object is not deleted from the list of map objects. You can re-enable the display of this object at a later time.

To enable or disable the display of a site on the main map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. If a line containing the name of the relevant site is not displayed in the list, this could be due to an applied filter based on site status. If this is the case, enable the display of all sites by clicking **All statuses** or click the name of the status that was assigned to the relevant site.
5. Move your cursor over the line containing the site name and click the button.

   After this operation is performed, the brightness of the icon in the button changes.

To enable or disable the display of a Server or sensor on the site map:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. Click the line containing the name of the relevant site.

   The site map opens.
5. Click **Show list of Servers**.

   A window containing the site name will appear in the right part of the section.
6. Select the **In site** tab.
7. If a line containing the relevant Server is not displayed in the list, this could be due to an applied filter based on Server status. If this is the case, enable the display of all Servers by clicking **All statuses** or click the name of the status that was assigned to the relevant Server.
8. If there are sensors associated with the Server and you want to enable or disable the display of these sensors, expand the **Sensors** list in the line containing the name of the relevant Server.
9. Move your cursor over the line containing the name of the relevant Server or sensor and click the button.

When you disable the display of a Server, this simultaneously enables the display of all sensors associated with this Server.

After this operation is performed, the brightness of the icon in the button changes.

Muting a Server in the Web Console

If the Kaspersky Security Center Web Console is receiving data from multiple Kaspersky Industrial CyberSecurity for Networks Servers and data from a specific Server does not require monitoring for a certain period of time (for example, during preventative maintenance and adjustment operations in the ICS), you can exclude this Server from monitoring ("mute" the Server). After you mute a Server, the Web Console will stop receiving data from this Server and will assign the *Muted* status to it. However, the Kaspersky Security Center Administration Server will continue receiving and saving data from this Server (including events).

The Server will remain muted until you re-enable monitoring for this Server ("unmute" the Server).

Servers can be muted and unmuted only by Kaspersky Security Center users who have been granted access permissions corresponding to the Administrator role in Kaspersky Industrial CyberSecurity for Networks.

To mute or unmute a Server:

1. Log in to the Kaspersky Security Center Web Console using an account that has Administrator privileges in Kaspersky Industrial CyberSecurity for Networks.
2. Select **KICS for Networks** → **Map**.
3. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
4. Click the line containing the name of the relevant site.

   The site map opens.
5. Click **Show list of Servers**.

   A window containing the site name will appear in the right part of the section.
6. Click the line containing the name of the relevant Server.

   A window containing detailed information about the Server will appear in the right part of the section.
7. If you want to mute the Server, click **Mute**. If the Server was already muted and you want to unmute it, click **Unmute**.
8. In the confirmation prompt window, click **OK**.

Viewing information about Servers on maps

The statuses of Kaspersky Industrial CyberSecurity for Networks Servers affect the colors of the displayed icons for Servers and the icons of sites on maps in the **KICS for Networks** → **Map** section of the Web Console. If icons of sensors are displayed on a site map, the colors of these icons depend on the current state of the nodes containing the sensors. This lets you keep track of the statuses of Kaspersky Industrial CyberSecurity for Networks components based on the colors of icons representing the objects on maps.

If necessary, you can view detailed information about each Server. The detailed information window provides the main data on the current state of the Server, information about installed updates of application modules and databases, data on hardware resource usage, and license key details.

To view detailed information about a Server:

1. Select **KICS for Networks** → **Map**.
2. Click **Show list of sites**.

   The **Sites** window will appear in the right part of the section.
3. Click the line containing the name of the relevant site.

   The site map opens.
4. Click **Show list of Servers**.

   A window containing the site name will appear in the right part of the section.
5. Click the line containing the name of the relevant Server.

   A window containing detailed information about the Server will appear in the right part of the section.
6. If you want to go to the web interface page of the Server, click **Go to Server**.

   The browser will open a tab showing the Server name that was defined during startup configuration of the application after installation.

Troubleshooting

This section contains a description of possible problems in the operation of Kaspersky Industrial CyberSecurity for Networks and methods for resolving them.

An application component cannot be installed on a selected node

Problem

During centralized installation of application components, there is a message stating that a node is unavailable for component installation due to failure to connect over the SSH protocol. The component is not installed on this node.

Solution

Centralized installation of an application component is impossible if the address information or network name of the computer was changed after configuring access over the SSH protocol on the node where the component will be installed. To centrally install the application component, you must restore access to the remote computer over the SSH protocol.

To restore access over the SSH protocol and install the application component:

1. On the computer from which the centralized installation of application components is performed, update the key used for connecting to the node over the SSH protocol. To do so, sign in to the system using the account credentials of the user account used to install the application, and enter the following command in the operating system console:

   ```
   sudo ssh-keygen -R <node IP address>
   ```

2. Reinstall the application with the same installation settings. During reinstallation, make sure that there is no message stating that the node is unavailable for component installation.

Application problems detected

Problem

When connected to the Server through the web interface, the upper part of the application web interface menu displays a red icon next to the button.

Solution

This state of Kaspersky Industrial CyberSecurity for Networks signifies that one of the application processes is malfunctioning.

To restore operation of the application:

1. Wait 20-30 seconds.

   The application may resume normal operation automatically. If the application resumes normal operation, the red icon will no longer be displayed.

2. If the malfunction persists, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

New application message

Problem

A new application message appears under **Settings** → **Application messages**.

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 **Settings** → **Application messages** by clicking when a red or yellow icon is displayed next to it.

Solution

An application message means that some event occurred in the application.

Read the concise information in the message under **Settings** → **Application messages**. Based on this information, you can make a decision on the necessary actions.

The next steps depend on the message status. The following statuses are available for messages:

- *Normal operation* – in most cases, the message does not require a response. However, there may be situations requiring additional clarification of the circumstances. For example, this may be necessary when you receive a message about the successful application of a security policy when you do not know why this action was taken.
- *Unknown*, *Malfunction* – if the message just recently appeared, wait 20–30 seconds and check the current state of the application.
- *Moderate malfunction*, *Critical malfunction* or *Fatal malfunction* – the application is malfunctioning. If the issue could not be resolved, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

Not enough free space on hard drive

Problem

There is not enough free space on the computer hard drive where the Application Server or sensor is installed.

Solution

The computer must meet the hardware and software requirements to ensure proper functioning of application components.

For the application to function correctly:

1. On the hard drive of the computer, free up sufficient space to satisfy the minimum free disk space requirements.
2. Restart the services supporting operation of application components.

An error occurs when enabling a monitoring point

Problem

After the monitoring point switches to *Enabled*, a status of *Error* is displayed. As a result, the node associated with this monitoring point will display a status of *Operation disrupted*. The list of notifications about application operating issues also shows a message regarding disrupted operation due to detected issues at the monitoring point.

Solution

An *Error* status of the monitoring point may be associated with an unsupported operational state of a network interface. For successful completion of a scan when a monitoring point is enabled, the network interface must have the *UP* operational state. If the network interface is in a different operational state. such as *UNKNOWN*, the application assigns a status of *Error* to the monitoring point because of possible problems when receiving or processing network packets.

You can use the `ip link` command to check the current operational state of a network interface on a node computer. Information about the current operational state is displayed in the string containing the name of the interface in the following format: `state <state>`. The most likely operational states on a problematic network interface are as follows:

- *DOWN*. In this case, you can switch the interface to the *UP* operational state by using the following command:

  ```
  sudo ip link set <interface name> up
  ```

- *UNKNOWN*. This operational state may be due to an incorrectly added interface. For example, network interfaces that were added by default on a VMware™ virtual machine may operate in the *UNKNOWN* state. In this case, it is recommended to re-add (create) a network interface with the correct settings by using the corresponding resources for managing network interfaces.

When the network interface switches to the *UP* operational state, check the status of the monitoring point added to this network interface. If the monitoring point is still displayed with a status of *Error*, disable and then re-enable this monitoring point.

No traffic at monitoring point

Problem

The application has registered an event whose description contains the following text: `No traffic at monitoring point`. The event description includes the duration of the absence of traffic, the name of the monitoring point, and the network interface that is not receiving traffic.

Solution

For traffic to arrive at the monitoring point, the following conditions must be met:

- The monitoring point is enabled, and its current status is *OK*.
- On the network interface of the monitoring point, the network cable is connected to the Ethernet port.
- The rate of incoming traffic is more than 0 bps at the network interface of the monitoring point.

You can view information about monitoring points and network interfaces when connected to the Server through the web interface under **Settings** → **Deployment**.

If the displayed rate of incoming traffic is 0 bps at the network interface of the monitoring point, verify that the following conditions are met:

- The network interface of the monitoring point is correctly configured in the operating system.
- When the network interface is connected to the industrial network switch, transmission of mirrored traffic through the connection port (SPAN) must be correctly configured on the network switch.

Traffic is not being loaded for events or incidents

Problem

Cannot load traffic for the selected events and/or incidents. The table of events either does not display the tools for loading traffic (for example, **Download traffic** is missing from the details area when one event is selected), or displays the message `No traffic for the selected events` (when attempting to load traffic).

Solution

Saved traffic for the selected events and/or incidents may be missing for one of the following reasons:

- The traffic was not saved.
- The traffic was deleted from the database.
- Traffic dump files were deleted.

The application saves traffic during event registration if the saving of traffic is enabled for the specific type of event. By default, saving of traffic is disabled for all event types. You can enable and configure the saving of traffic for relevant event types.

The application deletes saved traffic for registered events when one of the traffic storage limits is reached (for example, upon reaching the maximum volume of saved traffic in the database). Traffic packets that were saved before other packets are deleted from the database. If saved traffic is deleted too quickly and you do not have time to load it for relevant events, you can increase the maximum values of traffic storage settings.

When the limit is reached for stored traffic dump files, the application deletes temporary traffic dump files that were saved earlier than other files. If traffic dump files are being deleted faster than you are able to load traffic from these files, you can increase the maximum values of the traffic dump file storage settings or connect external storage on nodes.

Preventative maintenance and adjustment operations on the ICS

Problem

Preventative maintenance and adjustment operations on the ICS can create a large number of important and critical events in Kaspersky Industrial CyberSecurity for Networks.

Solution

While conducting preventive maintenance and adjustment operations, you can select one of the following options for resolving this problem:

- Leave all monitoring points and all technologies enabled on the Server and on application sensors. In this case, when viewing information about events and interactions of devices, take into account the time and list of preventive maintenance and adjustment operations to be conducted.
- Disable monitoring points or disable the use of technologies on monitoring points that receive traffic from industrial network segments where preventative maintenance and adjustment operations will be conducted. For example, if the work will be conducted in only one shop, you can disable the monitoring point that receives traffic from this shop and leave all other monitoring points enabled.
- Disable all monitoring points on all nodes that have application components installed. You can select this option if preventative maintenance and adjustment operations are to be conducted throughout the entire industrial network.

If you have disabled monitoring points or technologies, to resume control of the protected ICS you need to re-enable the monitoring points or technologies immediately after completion of preventative maintenance and adjustment operations.

Bear in mind that intruders may attempt to gain unauthorized access to the network during maintenance and commissioning operations on the ICS. Follow the security regulations and procedures in place at your enterprise when deciding to disable monitoring points or technologies.

If the composition or settings of the industrial network equipment were changed while conducting preventative maintenance and adjustment operations (for example, MAC addresses and IP addresses were changed), make the appropriate changes for Process Control, Interaction Control, and Asset Management. For example, you can configure the technology learning mode for the corresponding monitoring points.

Unexpected system restart

Problem

Unexpected restart of a computer hosting a component of Kaspersky Industrial CyberSecurity for Networks.

Solution

Wait for the computer restart 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 supporting operation of application components. If the problem is not resolved after the restart, please contact Kaspersky Technical Support. Be prepared to submit process logs of Kaspersky Industrial CyberSecurity for Networks and other system data when requested by Technical Support representatives. Process logs are located in the folders that are listed in the Folders for storing application data article. Root privileges in the operating system are required for providing access to logs.

Connector and remote connection functionality is unavailable after changing or adding the Server IP address

Problem

If the IP address for connecting via the web server has been changed or added on the Server machine, the connectors cannot connect to the Server at the new IP address due to certificate validation errors. Device scanning with application sensors is unavailable when using the **Remote connection** polling method.

Solution

To use a new Server IP address, you need to replace the main Server certificate used for securing connections with connectors and application component services.

After the main Server certificate is replaced, the old application sensor certificates are invalidated, which terminates any sensor-Server connections. To resume connections as part of the certificate renewal procedure, you will need to re-add and reconnect all sensors. You will also need to update the certificates used for connecting connectors.

Updates from the Kaspersky Security Center Administration Server are not received

Problem

When starting the database and application module update process with the selected update source, the **Kaspersky Security Center Administration Server** displays the message: `Update installation failed due to an error that interrupted the process.`

Solution

Downloading updates from the Kaspersky Security Center Administration Server is possible if the conditions for communication between Kaspersky Industrial CyberSecurity for Networks and Kaspersky Security Center are met. If any of the conditions is not fulfilled, ensure that they get fulfilled. For example, if the current version of the Kaspersky Industrial CyberSecurity for Networks administration plug-in for Kaspersky Security Center is not installed, install the plug-in.

In certain cases, update installation errors may be associated with inability to download updates from the Kaspersky Security Center repository. If updates for Kaspersky Industrial CyberSecurity for Networks have been uploaded to the update repository but are not available for download, you can perform the steps to clear the repository as described in the Kaspersky Security Center Knowledge Base.

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

Problem

If the settings from a backup copy were not restored after reinstalling the Kaspersky Security Center Administration Server, the Kaspersky Security Center Administration Console does not show the computer on which Kaspersky Industrial CyberSecurity for Networks is installed.

Solution

To restore synchronization of Network Agent, you can restore the settings of the Kaspersky Security Center Administration Server by using the klbackup utility. The klbackup tool is included in the Kaspersky Security Center distribution package. For detailed information on backup copying and restoring the settings of the Kaspersky Security Center Administration Server, please refer to the Kaspersky Security Center Help system.

If for some reason it is not possible to restore the settings of the Kaspersky Security Center Administration Server using the klbackup utility, you can restore synchronization of Network Agent by using the klmover utility that is included in Network Agent.

To use the klmover utility to restore synchronization of Network Agent:

1. On the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server, open the operating system console and go to the folder /opt/kaspersky/klnagent64/bin/.

2. Enter the following command in the command line:

   ```
   sudo ./klmover -address <IP address or computer name>
   ```

   where `<IP address or computer name>` is the IP address or name of the computer with Kaspersky Security Center.

3. After the klmover utility finishes, check the connection of Network Agent to the Kaspersky Security Center Administration Server. To do so, type the following command in the command line:

   ```
   sudo ./klnagchk
   ```

   The screen will display information about the connection to the Administration Server.

After Network Agent synchronization is successfully restored, the Kaspersky Security Center Administration Console will show the computer on which Kaspersky Industrial CyberSecurity for Networks is installed.

Unable to connect to the Server through the web interface

Problem

When attempting to connect to the Server, the Kaspersky Industrial CyberSecurity for Networks web interface page does not load.

Solution

Possible situations:

- There is no network access to the Kaspersky Industrial CyberSecurity for Networks Server computer that has the web server installed. Check the connection with the computer based on the specified Server name (for example, using the `ping` command).

- Incorrect data has been entered into the browser address bar. Enter the IP address or computer name of the Server that was specified for the web server under **Settings** → **Connection servers**. If the default port 443 is set, you do not have to specify the port number. If a different port number is specified, enter the full address in the `https://<Server name>:<port>` format in the address bar.

- JavaScript is disabled in the browser. A message about this is displayed on the connection failure warning page. In the browser settings, enable the execution of JavaScript and refresh the page.
- Access to the Server computer is blocked by the firewall. Properly configure the firewall that is being used.

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

Problem

When attempting to connect to a computer that has a Kaspersky Industrial CyberSecurity for Networks component installed, the browser displays a warning that the security certificate or the connection being established is not trusted. The contents of the warning depend on the specific browser being used.

Solution

The warning means that a self-signed certificate is being used on the web server.

You can temporarily use a self-signed certificate to connect to the Server (for example, when testing the operation of Kaspersky Industrial CyberSecurity for Networks). When using a self-signed certificate, in the browser warning window select the option that lets you continue connecting.

For permanent use, it is recommended to replace the self-signed certificate with a trusted one. You can replace the current certificate when updating the certificate for connecting to the Server through the web interface.

Contacting Technical Support

This section describes the ways to get technical support and the terms on which it is available.

How to get technical support

If you cannot find a solution to your issue in the application documentation or in other sources of information about Kaspersky Industrial CyberSecurity for Networks, we recommend that you contact Technical Support. Our Technical Support experts will answer your questions about installing and using Kaspersky Industrial CyberSecurity for Networks.

> Kaspersky provides support for Kaspersky Industrial CyberSecurity for Networks during the application's life cycle (please refer to the application life cycle page). Before contacting Technical Support, please read the technical support rules.

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

- visit Technical Support website
- Send a request to Kaspersky Technical Support through the Kaspersky CompanyAccount portal

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for organizations that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky experts via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky experts and store a history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single user account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese

- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website.

Collecting information for Technical Support

Kaspersky Technical Support experts may request your logs from Kaspersky Industrial CyberSecurity for Networks and other system data.

Logs are located on computers that have components of Kaspersky Industrial CyberSecurity for Networks installed. Information about the folders used for storing logs is provided in the Folders for storing application data article.

Root privileges in the operating system are required for providing access to logs.

Kaspersky Technical Support experts may also request additional data on the application components. This data can be obtaining by using the application components centralized installation script named kics4net-deploy-<application version number>.bundle.sh or by locally running the kics4net-gather-artefacts.sh script, which is located on the computer with the installed application component in the /opt/kaspersky/kics4net/sbin/ folder.

To get information about application components by using the kics4net-deploy-<application version>.bundle.sh script:

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

   ```
   bash kics4net-deploy-<application version number>.bundle.sh --gather-artefacts -<parameter> <directory 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.

- `<directory name>` – name of the directory used for copying archived data files.

Example

```
bash kics4net-deploy-<application version number>.bundle.sh --gather-artefacts -a /tmp/data_for_support
```

3. In the `SSH password` and `BECOME password` prompts, enter the password for the user account that was used to run the installation of application components.

Wait for completion of the script kics4net-deploy-<application version number>.bundle.sh. Upon successful completion, files will be created in the specified folder.

To obtain data on the application component installed on a computer by using the kics4net-gather-artefacts.sh script:

1. Log in to the system using the account credentials of a user account with root privileges.
2. Go to the /opt/kaspersky/kics4net/sbin/ folder and enter the following command for running the script to receive data on an application component:

```
bash kics4net-gather-artefacts.sh -<parameter> <directory 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.

- `<directory name>` – name of the directory used for copying archived data files.

Example

```
bash kics4net-gather-artefacts.sh -a /tmp/data_for_support
```

Wait for the kics4net-gather-artefacts.sh script to finish. Upon successful completion, files will be created in the specified folder.

Sources of information about the application

On the Kaspersky Industrial CyberSecurity for Networks page, you can view general information about the application, its functions and features.

The Online Help Guide contains information on administration of Kaspersky Industrial CyberSecurity for Networks. The Online Help Guide also provides information about the application's capabilities that users can utilize to accomplish common tasks.

Online Help includes documentation for the Kaspersky Industrial CyberSecurity for Networks API. This documentation serves as the Developer Guide for the Kaspersky Industrial CyberSecurity for Networks API. In the Kaspersky Industrial CyberSecurity for Networks API Developer Guide, you can find information on performing the following tasks:

- Preparing to use Kaspersky Industrial CyberSecurity for Networks API.
- Handling requests for receiving data from Kaspersky Industrial CyberSecurity for Networks and for sending data to the application.

If you cannot find a solution to an issue on your own, please contact Kaspersky Technical Support.

Appendices

This section provides information that complements the main document text with examples, reference information, and additional data.

Installing and configuring the CentOS Stream 9 operating system

This section describes the basic steps for installing and configuring the operating system on the computer where the Kaspersky Industrial CyberSecurity for Networks component will be installed: Server or sensor.

To install and configure the CentOS Stream 9 operating system:

1. Download the ISO image for installing the CentOS Stream 9 operating system from the official page of the CentOS project: https://centos.org/download/.
2. Create bootable media using the ISO image (such as on a USB drive).

   For example, you can create bootable media by using the Rufus utility.
3. Connect the bootable media to the computer where you want to install the operating system, and boot the computer from this media.
4. In the action selection menu, select **Install CentOS Stream 9**.
5. Select the localization language of the operating system.

   In the description of further actions, we use English as our chosen localization language.
6. Set the date and time.
7. If necessary, open the **Keyboard Layout** window and select additional keyboard layouts.
8. In the **Software Selection** section of the main menu, leave the default value **Server with GUI**.
9. Click the **Installation Destination** section of the main menu, select the drive for installing the operating system, and set the **Storage Configuration** parameter to **Custom**.
10. At the next step, unlock the settings by clicking the **Click here to create partitions automatically** link and configure the settings so that the size of the /home partition is no more than 10-15 GB and the rest is allocated to the system (root) partition. Leave the default values for the boot and swap partitions.
11. Click the **Network & Host Name** section of the main menu and enter a name for the computer (for example: `kics4net1`).
12. Click the **Root Password** section of the main menu and enter the password for the root account.
13. Create a user with root privileges to manage the operating system. For this root account, select the **Make this user administrator** and **Require a password to use this account** check boxes.
14. In the main menu window, click the **Begin Installation** button and wait for the installation of the operating system to complete.

15. After the installation is complete and the computer restarts, log in with the credentials of the user you created.

16. Configure the settings of the network interfaces of the computer. To do so, open the quick configuration menu in the upper-right corner of the screen and do the following:

    a. Select the **Settings** option. In the opened window, go to the **Network** section.

    b. Configure the settings for the available network interfaces in sequence:

    - For the network interface that will be used for connections through the web interface and connections with other components of the Kaspersky Industrial CyberSecurity solution, select the **Connect automatically** and **Make available to other users** check boxes, specify a static IPv4 address (**Manual**), disable use of the IPv6 protocol, and leave the security functions disabled on the **Security** tab.

    - For the network interface that will be used as a monitoring point, select the **Connect automatically** and **Make available to other users** check boxes, disable use of the IPv4 and IPv6 protocols, and leave the security functions disabled on the **Security** tab.

17. Restart the computer and log in with the account credentials of the user you created.

18. Open the operating system console and enter the commands for installing and configuring the required packages:

    - To install the glibc-langpack-zh package (required only for Kaspersky Industrial CyberSecurity for Networks 4.5.1):

      ```
      sudo dnf install glibc-langpack-zh
      ```

    - To install the chrony time synchronization package:

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

    - To disable the SELinux access control enforcement system:

      1. Open the `/etc/selinux/config` configuration file in a text editor (for example: in `mcedit`).

      2. Set the `SELINUX` parameter to `disabled`.

      3. Save and close the configuration file.

    - To install the dnf-utils package:

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

    - To install the compat-openssl package:

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

- To install the lttng-ust package with the LTTng library:

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

- To install the EPEL repository and the Python interpreter packages python3-psycopg2, python3-cryptography, and python3-paramiko that are required for the operation of connectors and data conversion scripts:

```
sudo dnf config-manager --set-enabled crb
sudo dnf install epel-release epel-next-release
sudo dnf install python3-psycopg2 python3-cryptography python3-paramiko
```

- To install the Postfix mail server (this may be required only on the computer that will perform Server functions):

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

- To update the Perl interpreter (this may be required only on the computer that will perform Server functions, and if the Kaspersky Security Center Network Agent is installed):

```
sudo dnf upgrade perl
```

19. Restart the computer.

Configuring time synchronization via the NTP and PTP protocols

This section describes the actions available for configuring time synchronization via NTP and PTP.

The time on nodes that have Kaspersky Industrial CyberSecurity for Networks components installed must be synchronized with a common source of time used by industrial network devices. For synchronization purposes, you can use the standard protocols known as Network Time Protocol (NTP) and Precision Time Protocol (PTP).

On the Server node, you must configure time synchronization regardless of how this component was installed (after centralized installation as well as after local installation).

On nodes hosting installed sensors, you must configure time synchronization in the following cases:

- Automatic time synchronization between the Server and sensors was not enabled during centralized installation of Kaspersky Industrial CyberSecurity for Networks.

- The sensor was installed locally using the kics4net-install.sh script.

The steps required for configuring time synchronization may differ depending on the version of the operating system and the specific protocol.

Configuring time synchronization via the NTP protocol in CentOS

To configure time synchronization via NTP in CentOS:

1. Open the operating system console.
2. Check the status of the standard time synchronization service known as chrony. To do so, enter the following command:

```
systemctl status chronyd
```

3. If the service is not found, enter the following commands to add the package and enable the service:

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

4. Open the service configuration file. To do so, enter the following command:

```
sudo mcedit /etc/chrony.conf
```

5. Specify the NTP servers that will be used for time synchronization. To specify the server, you only need to add the following string:

```
server <server name or IP address> iburst
```

6. Save and close the configuration file.
7. Restart the service. To do so, enter the following command:

```
sudo systemctl restart chronyd
```

8. Verify that the specified NTP servers are on the list of synchronization sources. To do so, enter the following command:

```
chronyc sources
```

Configuring time synchronization via the PTP protocol in CentOS

To configure time synchronization via PTP in CentOS:

1. Open the operating system console.
2. Check whether the linuxptp package is installed. To do so, enter the following command:

```
dnf list installed
```

3. If the linuxptp package is not installed, enter the following commands to add the package and enable the ptp4l time synchronization service:

```
sudo dnf install linuxptp
sudo systemctl enable ptp4l
sudo systemctl start ptp4l
```

4. Open the service configuration file. To do so, enter the following command:

```
sudo mcedit /etc/ptp4l.conf
```

5. Enter `1` for the `slaveOnly` parameter.
6. Save and close the configuration file.
7. Open the file containing the general settings for the service. To do so, enter the following command:

```
sudo mcedit /etc/sysconfig/ptp4l
```

8. In the `OPTIONS` string, specify the parameters as follows:

```
OPTIONS="-f <configuration file> -i <interface name> -S -s"
```

where:

- `-f <configuration file>` – default name and full path of the configuration file.
- `-i <interface name>` – name of the network interface that is used for time synchronization.
- `-S` – enables use of software-based timestamps. You can skip this parameter if you want to use hardware-based timestamps. However, first make sure that the equipment supports this capability.
- `-s` – enables subordinate time synchronization.

Example OPTIONS string

```
OPTIONS="-f /etc/ptp4l.conf -i eth0 -S -s"
```

9. Save and close the general settings file.

10. Allow use of ports 319 and 320 in the firewall for the UDP protocol. To do so, enter the following commands:

```
sudo firewall-cmd --permanent --add-port=319/udp
sudo firewall-cmd --permanent --add-port=320/udp
```

11. Restart the firewall service. To do so, enter the following command:

```
sudo systemctl restart firewalld
```

12. Restart the time synchronization service. To do so, enter the following command:

```
sudo systemctl restart ptp4l
```

Supported ASDU types identification in protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards

This article presents the ASDU types identification that are supported in Kaspersky Industrial CyberSecurity for Networks (see the table below). The listed types of frames are processed during Deep Packet Inspection on devices that interact over protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards.

Types of frames in protocols of the IEC 60870-5-104 and IEC 60870-5-101 standards

Frame type ID	Operation	Description	Type of main value / system commands
1. Process information in the monitoring direction			
<1>	M_SP_NA	Single-point information	bool (0 – OFF, 1 – ON)
<2>	M_SP_TA	Single-point information (with time tag)	bool (0 – OFF, 1 – ON)
<3>	M_DP_NA	Double-point information	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<4>	M_DP_TA	Double-point information (with time tag)	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<5>	M_ST_NA	Step position information	int8 (-64 … +64)
<6>	M_ST_TA	Step position information (with time tag)	int8 (-64 … +64)
<7>	M_BO_NA	String of 32 bits	unsigned int32
<8>	M_BO_TA	String of 32 bits (with time tag)	unsigned int32
<9>	M_ME_NA	Measured value, normalized value	float
<10>	M_ME_TA	Measured value, normalized value (with time tag)	float
<11>	M_ME_NB	Measured value, scaled value	float
<12>	M_ME_TB	Measured value, scaled value (with time tag)	float
<13>	M_ME_NC	Measured value, short floating point number	float
<14>	M_ME_TC	Measured value, short floating point number (with time tag)	float
<15>	M_IT_NA	Integrated total	int32
<16>	M_IT_TA	Integrated total (with time tag)	int32

Frame type ID	Operation	Description	Type of main value / system commands
<17>	M_EP_TA	Event of protection equipment (with time tag)	unsigned int8 (0 – Indeterminate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<18>	M_EP_TB	Packed start events of protection equipment (with time tag)	unsigned int8 (Set of bits in accordance with the standard)
<19>	M_EP_TC	Packed output circuit information of protection equipment (with time tag)	unsigned int8 (Set of bits in accordance with the standard)
<20>	M_PS_NA	Packed single-point information with status change detection	unsigned int16
<21>	M_ME_ND	Measured value, normalized value without quality descriptor	float
<30>	M_SP_TB	Single-point information (with time tag CP56Time2a)	bool (0 – OFF, 1 – ON)
<31>	M_DP_TB	Double-point information (with time tag CP56Time2a)	unsigned int8 (0 – Indeterminate or intermediate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<32>	M_ST_TB	Step position information (with time tag CP56Time2a)	int8 (-64 ... +64)
<33>	M_BO_TB	String of 32 bits (with time tag CP56Time2a)	unsigned int32
<34>	M_ME_TD	Measured value, normalized value (with time tag CP56Time2a)	float
<35>	M_ME_TE	Measured value, scaled value (with time tag CP56Time2a)	float
<36>	M_ME_TF	Measured value, short floating point number (with time tag CP56Time2a)	float
<37>	M_IT_TB	Integrated totals (with time tag CP56Time2a)	int32
<38>	M_EP_TD	Event of protection equipment (with time tag CP56Time2a)	unsigned int8 (0 – Indeterminate, 1 – OFF, 2 – ON, 3 – Indeterminate)
<39>	M_EP_TE	Packed start events of protection equipment (with time tag CP56Time2a)	unsigned int8 (Set of bits in accordance with the standard)
<40>	M_EP_TF	Packed output circuit information of protection equipment (with time tag CP56Time2a)	unsigned int8 (Set of bits in accordance with the standard)
2. Process information in the control direction			
<45>	C_SC_NA	Single command	bool (0 – OFF, 1 – ON)
<46>	C_DC_NA	Double command	unsigned int8 (0 – Unallowed, 1 – OFF, 2 – ON, 3 – Unallowed)
<47>	C_RC_NA	Regulating step command	unsigned int8 (0 – Unallowed, 1 – Next step UP, 2 – Next step DOWN, 3 – Unallowed)
<48>	C_SE_NA	Setpoint command, normalized value	float
<49>	C_SE_NB	Setpoint command, scaled value	float
<50>	C_SE_NC	Setpoint command, short floating point number	float
<51>	C_BO_NA	String of 32 bits	int32
<58>	C_SC_TA	Single command (with time tag CP56Time2a)	bool (0 – OFF, 1 – ON)
<59>	C_DC_TA	Double command (with time tag CP56Time2a)	unsigned int8 (0 – Unallowed, 1 – OFF, 2 – ON, 3 – Unallowed)
<60>	C_RC_TA	Regulating step command (with time tag CP56Time2a)	unsigned int8 (0 – Unallowed, 1 – Next step UP, 2 – Next step DOWN, 3 – Unallowed)
<61>	C_SE_TA	Setpoint command, normalized value (with time tag CP56Time2a)	float
<62>	C_SE_TB	Setpoint command, scaled value (with time tag CP56Time2a)	float
<63>	C_SE_TC	Setpoint command, short floating point number (with time tag CP56Time2a)	float

Frame type ID	Operation	Description	Type of main value / system commands
<64>	C_BO_TA	String of 32 bits (with time tag CP56Time2a)	int32
3. System information in the monitoring direction			
<70>	M_EI_NA	End of initialization	END OF INITIALIZATION system command
4. System information in the control direction			
<100>	C_IC_NA	Interrogation command	INTERROGATION system command
<101>	C_CI_NA	Counter interrogation command	COUNTER INTERROGATION system command
<102>	C_RD_NA	Read command	READ system command
<103>	C_CS_NA	Clock synchronization command	CLOCK SYNCHRONIZATION system command
<104>	C_TS_NA	Test command	TEST system command
<105>	C_RP_NA	Reset process command	RESET PROCESS ACTIVATION / RESET PROCESS CONFIRMATION system commands
<106>	C_CD_NA	Delay acquisition command	DELAY ACQUISITION system command
<107>	C_TS_TA	Test command (with time tag CP56Time2a)	TEST WITH TIME TAG system command
5. Parameters in the control direction			
<110>	P_ME_NA	Parameter of measured value, normalized value	float
<111>	P_ME_NB	Parameter of measured value, scaled value	float
<112>	P_ME_NC	Parameter of measured value, short floating point number	float
<113>	P_AC_NA	Parameter activation	PARAMETER ACTIVATION system command
6. File transfer			
<120>	F_FR_NA	File ready	Not processed
<121>	F_SR_NA	Section ready	Not processed
<122>	F_SC_NA	Call directory, select file, call file, call section	CALL DIRECTORY, SELECT FILE, CALL FILE, CALL SELECTION system command
<123>	F_LS_NA	Last section, last segment	Not processed
<124>	F_AF_NA	Confirm file, confirm section	Not processed
<125>	F_SG_NA	Segment	Not processed
<126>	F_DR_TA	Directory	Not processed

Loading, processing, and managing device and tag configurations with support for IEC 61850 standard protocols

The technologies for analyzing industrial network traffic used in Kaspersky Industrial CyberSecurity for Networks provide basic information about the parameters and interactions of devices supporting protocols of the IEC 61850: IEC 61850-8-1 (GOOSE, MMS) standard. However, to get and save the most complete data about these devices, including tags in their original structured format, it is recommended to load the contents of files prepared in accordance with the IEC 61850-6 standard into the application. The contents of such files are loaded by importing projects for IEC 61850 devices.

When importing a project for IEC 61850 devices, Kaspersky Industrial CyberSecurity for Networks checks the syntax and format of the contents of the project files and analyzes the device configurations in the project for compliance with the requirements and recommendations of the IEC 61850 standard. After successfully importing a project, the application analyzes the traffic for compliance with the imported configuration. If the traffic displays interactions that deviate from the saved configuration (device interactions or transmitted settings do not match the descriptions in the configuration), the application registers events.

This way, the built-in tools for processing and managing configurations of IEC 61850 devices let you use Kaspersky Industrial CyberSecurity for Networks both as an application for protection against information security threats and as a tool for scanning files containing configuration descriptions. Based on the data from the files, the application allows you to detect errors and flaws in the design of sets of IEC 61850 devices. You can eliminate the identified errors and design flaws step by step.

Supported project types and protocol processing modules are updated along with updates to application modules and databases. You need to install updates to use all the features supported by the application for analyzing device configurations and analyzing traffic over IEC 61850 protocols.

The scenario for bringing a project into compliance with the IEC 61850 standard consists of the following steps:

1. **Importing a project for IEC 61850 devices into Kaspersky Industrial CyberSecurity for Networks.**

   At this step, you must import a project for IEC 61850 devices. Device configurations in the imported project must be described in SCL (System Configuration Language) and saved in one or several files used in accordance with the IEC 61850 standard. The SCL file types *.SCD, *.CID, and *.ICD are supported for importing this type of project.

   At the end of the import process, the application provides the capability to view a report on the results. To view the report, you must open the list of background operations by clicking the button in the application web interface menu and then click the **Display report** button after the import process completes.

   If errors or deficiencies (inconsistencies) are detected during the scan and analysis of the imported file, information about them is displayed in the report window under the following sections:

   - **Syntax and formatting errors**.
   - **Non-conformity with the standard** (no more than 100 detected non-conformities are displayed).

   If the report window does not contain any of the specified sections, you can proceed to step 3. Otherwise, carefully read the lists of errors and inconsistencies in the report window and proceed to step 2.

2. **Resolving errors and inconsistencies according to the import report**

   Errors and inconsistencies detected during an import may vary in their importance. Some errors (for example, syntax errors of different revisions) make it impossible to load the file and block the import of the entire contents of the project. Other errors and inconsistencies can be caused both by logical errors in the imported project and by the specific settings of the equipment being used (if the operational capabilities of the equipment let you set parameters for it without adhering to certain recommendations for using the IEC 61850 standard). The application displays the appropriate warnings for these errors and inconsistencies in the import report.

   After reviewing the lists of errors and inconsistencies found during the import, you need to decide on the necessary improvements to make in the project. Use the appropriate software tools to resolve the errors and inconsistencies.

   If you have made any revisions or additions to the project, save the project files and perform step 1 again to import the updated files. If project revisions are not required, skip to step 3.

3. **Scanning objects that were created in Kaspersky Industrial CyberSecurity for Networks as a result of the project import**

At this step, you need to check the changes in the application after the import and perform additional actions with the objects in the application if necessary.

If the imported project contains the relevant data, the application performs the following actions:

- Adds new devices (or updates existing devices) while indicating the address information of the participants of network interactions.
- Adds Process Control settings for devices and saves the following in these settings:
  - Monitored system commands
  - Subscriptions and data blocks for the MMS and GOOSE protocols
- Adds tags of the MMS and GOOSE protocols in the original structured format of tags.
- Generates Interaction Control rules based on information about devices in the imported configuration.

For tags in structured format, it is not possible to define conditional Process Control rules to track values. If you want to check the values of tags using the application, you can use rules with Lua scripts for this purpose.

4. **Tracking events registered upon detection of deviations from the saved configuration in traffic**

The application uses a saved configuration to analyze industrial network traffic. If the traffic displays interactions that deviate from the saved configuration (device interactions or transmitted settings do not match the descriptions in the configuration), the application registers events based on Network Integrity Control and Command Control technologies.

When analyzing interactions over the IEC 61850: GOOSE protocol, the application registers events in the following cases:

- Inconsistencies in the MAC addresses of the sources and recipients of messages are detected.
- Factory configurations are detected (identical goID in GOOSE messages).
- Inconsistencies in ConfRev versions are detected.
- Inconsistencies in the statuses of GOOSE messages are detected.
- Inconsistencies in the main parameters of GOOSE message packets are detected.
- Inconsistencies in signal quality settings are detected.
- Inconsistencies in the message transmission sequence are found.
- A GOOSE message from an undescribed device is detected.
- An undescribed GOOSE message from a described device is detected.
- Changes in the structure of a data packet in a GOOSE message are detected.
- Inconsistencies in the use of the VLAN ID in GOOSE messages are detected.
- Inconsistencies between tag values and created Process Control rules are detected.

When analyzing interactions over the IEC 61850: MMS protocol, the application registers events in the following cases:

- Inconsistencies in IP or MAC addresses are detected (taking into account the interactions through routers).
- Duplicate names/addresses are detected.
- Inconsistencies in ConfRev versions are detected.
- Inconsistencies in the sequence of executed system commands are detected.
- Inconsistencies between tag values and created Process Control rules are detected.
- Inconsistencies in client-to-server connection methods (read/write or by subscription) are detected.

The duration of the event tracking phase depends on the frequency of device interactions and changes in operating modes within the industrial process. If your assessments indicate that all monitored devices have performed their intended operations and the application does not register any events for the above reasons, the scenario for bringing the project into compliance with the IEC 61850 standard can be considered complete. Otherwise, if events are registered, go to step 5.

5. **Fine-tuning the project to eliminate deviations from the saved configuration**

   When investigating the reasons for event registration, first verify the absence of information security threats and the absence of industrial process violations.

   After you are convinced that the events were registered due to errors or inconsistencies in the saved configuration, you need to decide on the necessary improvements to make in the project. Use the appropriate software tools to resolve the errors and inconsistencies.

   If you have made any modifications to the project, save the project files and repeat the steps in this scenario starting with step 1.

After taking all the necessary actions to bring the project into compliance with the IEC 61850 standard, you can use all of the functions of Kaspersky Industrial CyberSecurity for Networks in monitoring mode. However, it is recommended to regularly assess the security and performance of the industrial network infrastructure by employing the following application features:

- Monitor network sessions and perform online monitoring to assess current network congestion (including by using the **Traffic** and **Tags** widgets).
- Use Asset Management, Interaction Control, Rule-based Network Anomaly Detection and Intrusion Detection to monitor the appearance of devices with new addresses on the network.
- Monitor events to track undescribed messages registered in events based on Command Control technology and to track faults and network errors registered in events based on Intrusion Detection technology (system event type codes 4000005100, 4000005101, 4000005102, 4000005103, and 4000002701) and in events based on Asset Management technology (system event type code 4000005005).

Sending Kaspersky Industrial CyberSecurity for Networks events to SIEM systems

This section describes events sent to SIEM systems.

In Kaspersky Industrial CyberSecurity for Networks, you can use a connector to send data to a SIEM system server. After you add a connector, you need to configure forwarding of events through this connector.

The contents and order in which information is displayed about events forwarded to a SIEM system may differ from the data displayed on the **Events and incidents** tab in the **Events** of the Kaspersky Industrial CyberSecurity for Networks Server web interface.

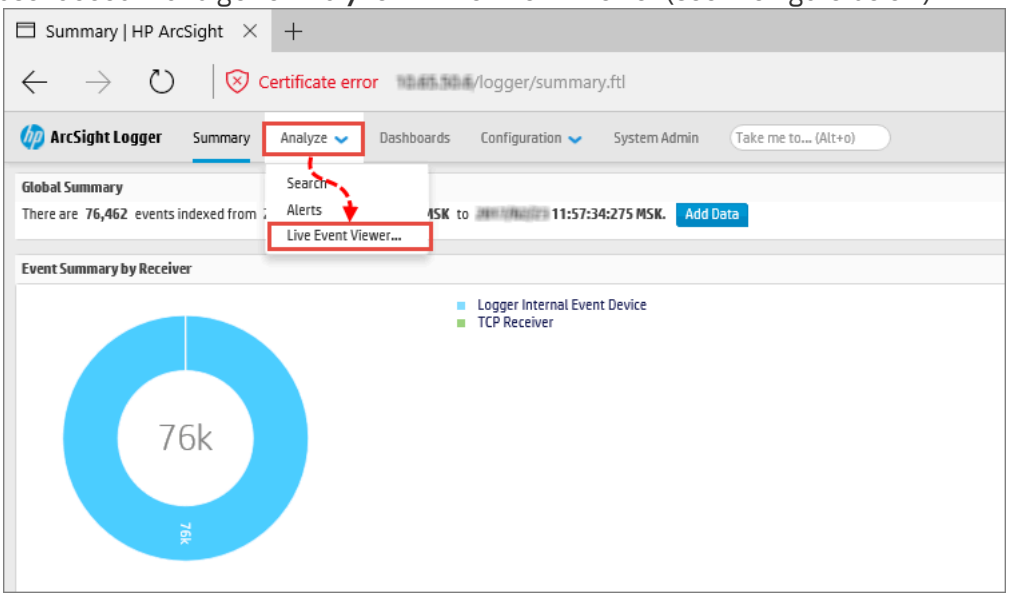
Verifying event forwarding using an HP ArcSight system (as an example)

To verify event forwarding using an HP ArcSight system as an example:

1. Make sure that a channel is configured for receiving messages from Kaspersky Industrial CyberSecurity for Networks using the standard tools of the HP ArcSight system.

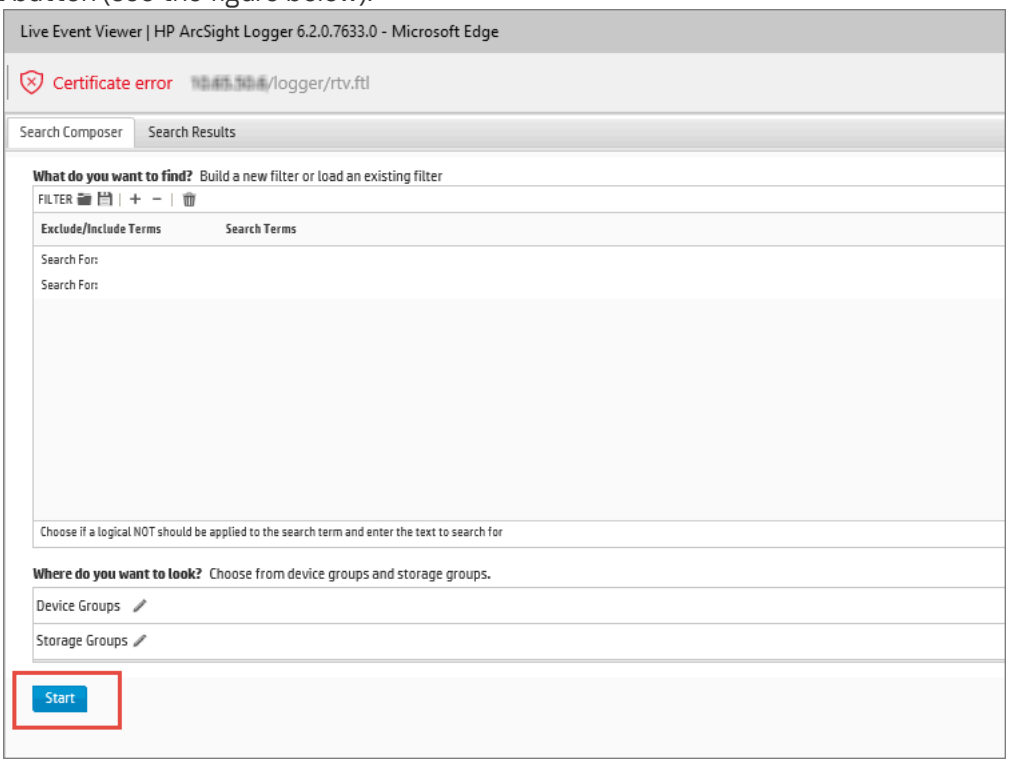
2. Open your browser and enter the address of your HP ArcSight system.

3. Log in to your user account and go to **Analyze** → **Live Event Viewer** (see the figure below).



Opening the **Live Event Viewer** section in the HP ArcSight system

4. Click the **Start** button (see the figure below).



Starting **Live Event Viewer** in the HP ArcSight system

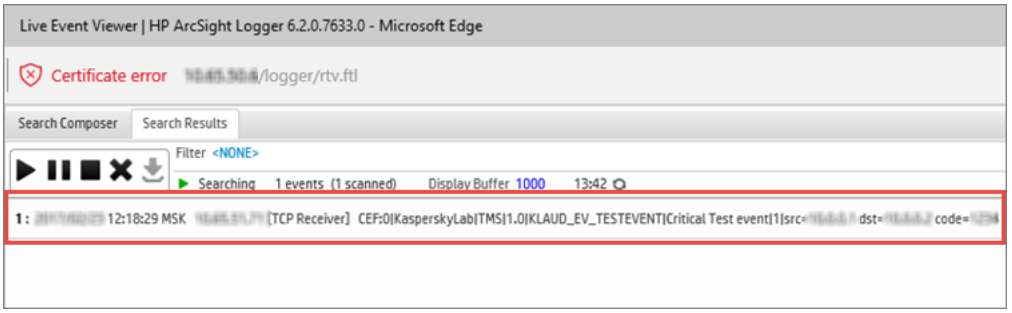
5. Open the command line interface and enter the following command to connect to the server over the Telnet protocol:

```
telnet <ArcSight server address> <port>
```

6. Send a test message in CEF format:

```
CEF:0|KasperskyLab|TMS|1.0|KLAUD_EV_TESTEVENT|Critical Test event|1|src=10.0.0.1 dst=10.0.0.2 code=1234
```

If there is a connection with the HP ArcSight system, the **Live Event Viewer** section will show an event whose contents match the message that was sent (see the figure below).



Verifying operation results

Format of messages forwarded to a SIEM system

The application transmits data to a SIEM system in CEF 20 format. The following internal structures are used for data transmission:

- `EventMessage` – for events.
- `ApplicationMessage` – for application messages.
- `AuditMessage` – for audit entries.

Received messages are not converted to the system log protocol format.

Format of the EventMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Event — corresponding field of the event in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Event	Description
dateTime	Start	Date and time (with precision down to the millisecond) when the event-triggering network packet was captured.
hostname	Kaspersky Industrial CyberSecurity for Networks Server address	Address of the Kaspersky Industrial CyberSecurity for Networks Server.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.5.0.247	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Event	Sent message type.
signatureId	Event type	Event type ID.
name	Title	Event description.
severity	Event severity level: • 9 – scores 8.0–10.0 • 6 – scores 4.0–7.9 • 3 – scores 0.0–3.9	Event severity level. Values from 3 to 9, where 9 is the most severe event.
score	Event score	Event score value.
extension	Indicated in the Extension Fields table	Determined individually for each type of message.

Date and time is sent in the following format: `YYYY-MM-DD T hh:mm:ss.ms Z`. Example: 2025-10-30T22:14:15.030Z – time of the event, which occurred on October 30, 2025 at 22 hours, 14 minutes, 15 seconds, and 030 milliseconds.

Contents of Extension Fields

The table below provides data in the following columns:

- Extension — field name in a message.
- Related events — events in which the specific field is sent.
- Description — field description.

Extension	Related events	Description
cnt	Common fields of events	Counter of the number of times an event is repeated after the event is registered.
dmac	Common fields of events	Destination MAC address.
dmacas	Common fields of events	Address space for the destination MAC address.
dpt	Common fields of events	Destination port.
dst	Common fields of events	Destination IP address.
das	Common fields of events	Address space for the destination MAC address (if additional address spaces are added to the application).
end	Common fields of events	Event end time.
smac	Common fields of events	Source MAC address.
smacas	Common fields of events	Address space for the source MAC address.
spt	Common fields of events	Source port.
src	Common fields of events	Source IP address.
srcas	Common fields of events	Address space for the source MAC address (if additional address spaces are added to the application).
start	Common fields of events	Event registration time.
technology	Common fields of events	Technology that was used to register the event.
triggeredRule	Common fields of events	Triggered rule.
protocol	Common fields of events	Protocol.
vlanId	Common fields of events	VLAN ID.
monitoringPoint	Common fields of events	Monitoring point whose traffic invoked registration of the event.
sourceIndustrialAddress	Common fields of events	Application-level address for the source.
destinationIndustrialAddress	Common fields of events	Application-level address for the destination.
eventIdentifier	Common fields of events	Event ID.
noTrafficDuration	No traffic at monitoring point	Period of no traffic.
tagId	Invalid tag type	Tag ID.
expectedTagType	Invalid tag type	Expected data type of tag.
actualTagType	Invalid tag type	Actual data type of tag.
ruleName	• Process Control rule violation • Intrusion Detection rule from the system set of rules was triggered	Rule name.
tags	Process Control rule violation	Tags.

msg	Intrusion Detection rule from the system set of rules was triggered	Message.
substitutedIpAddress	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	IP address of the source of network packets.
targetIpAddress	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	IP address of the destination of network packets.
attackStartTimestamp	• Signs of ARP spoofing detected in ARP replies • Signs of ARP spoofing detected in ARP requests	Start time of the activity showing signs of an attack.
ownerMac	• IP address conflict detected • New IP address detected • New device detected • New information received • Traffic detected from MAC address • MAC address added to device • IP address added to device	MAC address of owner.
ownerIp	• New device detected • MAC address added to device • IP address added to device • IP address conflict detected • New MAC address detected	IP address of owner.
challengerMac	IP address conflict detected	MAC address of challenger.
newIpAddress	New IP address detected	New IP address.
newMacAddress	New MAC address detected	New MAC address.
oldIpAddress	New IP address detected	Old IP address.
assetName	New device detected	Device name.

Device settings

The table below provides data on the settings of devices.

If one or two devices were identified for a detected interaction, Kaspersky Industrial CyberSecurity for Networks also sends known information about one or two devices to the SIEM system.

If multiple devices were identified for a detected interaction, the message is duplicated with different address information and different device settings (if the devices are different).

Extension	Device setting
srcAssetName	Name of the source device.
srcVendor	Vendor of the source device.
srcOS	Operating system of the source device.
srcNetworkName	Network name of the source device.
srcModel	Model of the source device.
dstAssetName	Name of the destination device.
dstVendor	Vendor of the destination device.
dstOS	Operating system of the destination device.

dstNetworkName	Network name of the destination device.
dstModel	Model of the destination device.

Format of the ApplicationMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Application message – corresponding field of the application messages in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Application message	Description
dateTime	Occurrence date and time	Date and time (to the millisecond) when the situation that caused the message logging was detected.
hostname	Address of Kaspersky Industrial CyberSecurity for Networks Server or sensor	Node address of Kaspersky Industrial CyberSecurity for Networks Nodes Server or sensor.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.5.0.247	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Application message	Sent message type.
severity	Application messages severity level: • 10 for the following statuses: *Moderate malfunction*, *Critical malfunction*, or *Fatal malfunction*. • 5 for the following statuses: *Unknown*, *Malfunction*. • 0 for the *Normal operation* status.	Application messages severity level. Values from 0 to 10, where 10 is the most severe message.
address	Node address	Address of the node from which the message originated.
systemProcess	Process name	Application process that invoked message registration.
msg	Message	Numerical identifier and text of the message.

Format of the AuditMessage structure

The table below provides data in the following columns:

- EventMessage — field name in a message.
- Audit message – corresponding field of the audit entry in Kaspersky Industrial CyberSecurity for Networks or a specific value.
- Description — field description.

EventMessage	Audit message	Description
dateTime	Occurrence date and time	Date and time (to the millisecond) when the situation that caused the audit entry logging was detected.

hostname	Kaspersky Industrial CyberSecurity for Networks Server address	Node address of Kaspersky Industrial CyberSecurity for Networks Server.
cefVersion	0	CEF version number.
deviceVendor	Kaspersky Lab	Vendor.
deviceProduct	Kaspersky Industrial CyberSecurity for Networks	Product name.
deviceVersion	Example: 4.5.0.247	Version of Kaspersky Industrial CyberSecurity for Networks.
messageType	Audit message	Sent message type.
address	User node	Address of the node where the registered action was performed.
user	User	Name of the user that performed the registered action.
action	Action	Registered action performed by the user.
result	Result	Result of the registered action (successful or unsuccessful).
msg	Description	Additional information about the registered action.

Changing Kaspersky Industrial CyberSecurity for Networks configuration settings using a script

In Kaspersky Industrial CyberSecurity for Networks, you can change the application configuration settings listed in the table below. Settings are edited with the help of the kics4net-params script, located at /opt/kaspersky/kics4net/sbin/ on the Server computer.

Kaspersky Industrial CyberSecurity for Networks configuration settings

Configuration setting (alternate name for setting)	Default value	Range of values	Description
`-t` (`--logon_session_timeout`)	600 minutes (equivalent to 10 hours)	From 1 to 43,200 minutes	Validity period for Server connection sessions via the web interface and authentication tokens in the Kaspersky Industrial CyberSecurity for Networks API. The value is presented in minutes.
`-l` (`--max_password_ttl_in_days`)	90 days.	From 1 to 366 days	The maximum password age requiring a password change. The value is expressed in days.
`-a` (`--attempts_to_login_limit`)	3	From 1 to 100	The number of failed login attempts that triggers a notification to the administrator.

You can use the kics4net-params script to view and adjust configuration settings.

To view the running configuration settings:

1. On the Server computer, log in to the system using the account credentials of a user account with root privileges that you want to use to run the kics4net-params script.

2. Go to the /opt/kaspersky/kics4net/sbin/ folder and enter the following command for running the script to view the currently defined value:

```
sudo python kics4net-params get -n <configuration setting>
```

where:

- `-n` disables display of the internal name used to represent the value in the application configuration. If the setting is undefined, the value is displayed together with the name (for example: `logon_session_timeout=<value>`).
- `<configuration setting>` is the configuration setting whose value will be displayed on the screen (mandatory setting).

Example command to display the maximum password age

```
sudo python kics4net-params get -n -l
```

To adjust configuration settings:

1. On the Server computer, log in to the system using the account credentials of a user account with root privileges that you want to use to run the kics4net-params script.
2. Go to the /opt/kaspersky/kics4net/sbin/ folder and enter the following command for running the script to change the value:

   ```
   python kics4net-params set -r <configuration setting>=<value>
   ```

   where:

   - `-r` enables automatic restart of application services on the Server computer after a new value is applied. If this parameter is not defined, you will have to manually restart the Server computer or restart services after the script is finished.
   - `<configuration setting>=<value>` is the new value for the configuration setting (mandatory setting).

   Example command to change the maximum password age

   ```
   sudo python kics4net-params set -r -l=100
   ```

Specifics of connecting Kaspersky Industrial CyberSecurity for Networks nodes as connection gateways in Kaspersky Security Center

You can use nodes with installed application components (Server and sensors) as connection gateways in Kaspersky Security Center. Distribution points act as gateways for connections to the Kaspersky Security Center Administration Server. The diagram of communication with managed devices using distribution points allows you to optimize database, application module, and Kaspersky application update traffic on the network and configure traffic restrictions for IP ranges in Kaspersky Security Center. If a Kaspersky Industrial CyberSecurity for Networks Server or sensor node provides the only available connection between the Administration Server and managed devices located on an isolated network, the connection gateway role on this node allows you to provide Administration Server network connectivity with these devices.

This article describes a scenario for configuring and scanning a Kaspersky Industrial CyberSecurity for Networks node to act as a connection gateway in Kaspersky Security Center. The scenario consists of the following steps:

1 Installing Network Agent on the node

Network Agent is installed automatically on the Kaspersky Industrial CyberSecurity for Networks Server node if the functionality for communication between the application and Kaspersky Security Center was added during Server installation. After adding the communication functionality, enable and configure the functionality in Kaspersky Industrial CyberSecurity for Networks.

> You must enable and configure the communication functionality in Kaspersky Industrial CyberSecurity for Networks before configuring Network Agent on the Server to act as a connection gateway. Enabling the communication functionality after configuring Network Agent on the Server resets the specified configuration settings and disables the connection gateway role on the node. In that case, to resume node operation as a connection gateway, repeat the steps in the scenario, starting with Network Agent configuration.

Network Agent is not installed on the sensor node by default during centralized or local installation of Kaspersky Industrial CyberSecurity for Networks components. If Network Agent is not installed on the sensor node, install it with the help of the klnagent64-<Network Agent version number>.x86_64.rpm package, which is saved in the directory named kics4net-release_<application version number>/linux-centos when preparing for installation of the application.

To install the Network Agent, do the following on the computer with the sensor installed:

1. Copy the klnagent64-<Network Agent version>.x86_64.rpm Network Agent installation package to any directory

2. In the operating system console, go to the folder containing package file, and enter the following command:

```
sudo rpm -i klnagent64-<Network Agent version number>.x86_64.rpm
```

Wait for the Network Agent installation process to finish.

2 Allowing the use of ports

At this step, you must allow the use of firewall ports on the Network Agent node computer. You can use the following commands to enable port use:

```
sudo firewall-cmd --permanent --add-port=13000/tcp
sudo firewall-cmd --permanent --add-port=13295/tcp
sudo systemctl restart firewalld
```

3 Configuring Network Agent

This step activates connection gateway mode on Administration Agent. When this mode is activated with subsequent addition of a node as a distribution point, Kaspersky Security Center changes the identification and authentication details for using this device as a connection gateway.

> Changes to credentials and authentication information require that for the new distribution point to be used as the connection gateway on a previously configured network, you reinstall Network Agent on all devices that you want to connect to the newly added connection gateway. This includes those devices that previously used the node as a connection gateway. Until Network Agent is reinstalled on these devices, they will not be able to connect to the newly added connection gateway.

To activate connection gateway mode on Network Agent, do the following on the node computer:

1. Run the post-installation script to configure the Network Agent local environment. To do so, enter the following command:

   ```
   sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

2. Please carefully read the End User License Agreement. To go to the next screens containing the text of the End User License Agreement, press **SPACE**.

3. When done viewing and if you fully agree with the terms of the End User License Agreement, accept the terms. To do so, enter `y`.

4. Enter the Administration Server name or IP address.

5. If needed, change the default ports for unencrypted and encrypted connections to the Administration Server.

6. Select a mode for connecting to the Administration Server. To do so, enter the appropriate character:

   `y`: secure connections via SSL

   `n`: unencrypted connections.

7. At the step where the Network Agent operation mode is requested, select **Use as connection gateway**.

8. Wait for the script to finish. Two to three minutes after the script finishes running, check the connection between Network Agent and the Administration Server. To do so, enter the following command:

   ```
   sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

The screen will display information about the connection to the Administration Server. If the configuration was applied successfully, the following messages will be displayed on the screen:

```
HostId: <ID as an alphanumeric sequence>
This host was installed as a connection gateway, but not yet registered on server
Connecting to server...OK
Connecting to the Administration Agent...OK
```

4 Adding a node as a distribution point in Kaspersky Security Center

The Kaspersky Industrial CyberSecurity for Networks node will begin acting as a connection gateway after it is added as a distribution point in Kaspersky Security Center. To do this, do the following:

1. Connect to the Kaspersky Security Center Administration Server.

2. In the console tree, open the context menu of the **Administration Server** node and select **Properties**.

3. In the Administration Server properties window, select the **Distribution points** section.

4. In the right part of the window, select **Manually assign distribution points** and click **Add**.

   The **Add distribution point** window opens.

5. To specify a device that will act as a distribution point, select the option to add a connection gateway and enter the IP address or computer name of the Kaspersky Industrial CyberSecurity for Networks node.

6. To specify the scope of the distribution point, select the **Administration group** option and specify the administration group whose devices will use the connection gateway.

7. After adding the node to the list of distribution points, make sure that a persistent connection with the Administration Server is enabled for the node. To do so, open the node properties window and check that the **Do not disconnect from the Administration Server** check box in the **General** section is selected. This check box must be selected automatically and must not be cleared or selected manually.

5 **Verifying a successful connection between Network Agent and Kaspersky Security Center**

You can verify that the steps involved in adding the connection gateway and distribution point were successful on the node computer. To do so, enter the following command:

```
sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

The screen will display information about the connection to the Administration Server. If the steps are completed successfully, the following messages are displayed on the screen:

```
Host is a connection gateway
Host is a distribution point
Connection with server: active
CG connection with server: active
```

Files for importing a universal project

You can use a universal-format project to import Process Control configurations for devices and tags into Kaspersky Industrial CyberSecurity for Networks. A universal project can be imported by using text files with delimiters (CSV files). CSV format is a text format for presentation of table data.

You can create data files using any method of your choice (for example, from SCADA systems). To import your created files into the application, you need to pack the files into a ZIP archive.

The set of files used for importing a universal project may consist of the following CSV files:

- devices.csv. Contains descriptions of devices.
- connections.csv. Contains descriptions of connections.

  A *connection* is a named link between a device, a set of device protocols, and a set of device tags relayed through such protocols.
- variables.csv. Contains descriptions of variables and tags for connections.
- enums.csv. Contains descriptions of enumerations for the IEC 61850 standard.
- datasets.csv. Contains descriptions of data sets for the IEC 61850 standard.
- iec61850_mms_reports.csv. Contains descriptions of reports for the IEC 61850: MMS protocol.

When using a Universal-format project, you cannot import IEC 61850 MMS and GOOSE tags in their original structured tag view. If a tag contains a field structure, each field of this structure must be described as a separate tag for the application. To add structured tags to the application, use the following specially designed project type: **project for IEC 61850 devices**.

When using data files, consider the following specifics:

- Data files must have UTF-8 encoding.
- The list of tags in the variables.csv file has the "connection" grouping attribute.
- You can specify several different protocols and addresses for one connection in the connections.csv file.
- A protocol can have one or several addresses.
- One device can have several connections with different sets of tags.
- 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.
- Rows containing the parameter values in the enums.csv and datasets.csv files are filled out only when describing enumerations and data sets for MMS and GOOSE protocols of the IEC 61850 standard. For other protocols, the enums.csv and datasets.csv files can contain only header rows. Please note that the enums.csv and datasets.csv files must be included in the set of files used for the import.

File with descriptions of devices: devices.csv

The file with descriptions of devices contains an enumeration of devices, their classes, and connection IDs. Connection ID in the device description file is specified in the connections description file and is used for linking protocols to the devices.

If you use different protocols with different sets of tags, you have to use several connections for one device. Connection IDs in each row of the devices.csv file have to be unique.

The file should begin with header strings containing the data needed for file processing.

Example header strings of the devices.csv file

```
'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 class code. The following codes are used:
    - 0 – SIEMENS SIMATIC S7-300
    - 1 – SIEMENS SIMATIC S7-400
    - 2 – SCHNEIDER ELECTRIC MOMENTUM
    - 3 – SCHNEIDER ELECTRIC M340
    - 4 – MITSUBISHI SYSTEM Q
    - 5 – ALLEN-BRADLEY CONTROL LOGIX 5000
    - 6 – SIEMENS SIPROTEC
    - 7 – IEC 61850 GOOSE, MMS device
    - 8 – IEC 60870-5-104 device
    - 9 – ABB RELION 670
    - 10 – GENERAL ELECTRIC RX3I
    - 11 – SIEMENS SIMATIC S7-1500
    - 12 – IEC 61850 SAMPLED VALUES device
    - 13 – SIEMENS SIPROTEC 6MD66
    - 14 – SIEMENS SIPROTEC 7SS52
    - 15 – SIEMENS SIPROTEC 7UM62
    - 16 – SIEMENS SIPROTEC 7SA52
    - 17 – SIEMENS SIPROTEC 7SJ64
    - 18 – SIEMENS SIPROTEC 7UT63

- 19 – GENERAL ELECTRIC MULTILIN B30
- 20 – GENERAL ELECTRIC MULTILIN C60
- 21 – EMERSON DELTAV
- 22 – SCHNEIDER ELECTRIC M580
- 23 – RELEMATIKA TOR 300
- 24 – EKRA 200 series
- 25 – EKRA BE2704 / BE2502
- 26 – OMRON CJ2M
- 27 – ABB AC 800M
- 28 – YOKOGAWA CENTUM
- 29 – CODESYS V3 based device
- 30 – DNP3 device
- 31 – OPC UA server
- 32 – ABB AC 700F
- 33 – SIEMENS SIMATIC S7-1200
- 34 – OPC DA server
- 35 – BECKHOFF CX series
- 36 – PROSOFT-SYSTEMS REGUL R500
- 37 – EMERSON CONTROLWAVE
- 38 – IEC 60870-5-101 device
- 39 – MOXA NPORT IA 5000 series
- 40 – I/O device
- 41 – ABB RELION REF615
- 42 – SIEMENS SIMATIC S7-200
- 43 – MODBUS TCP device
- 44 – SCHNEIDER ELECTRIC SEPAM 80 NPP
- 45 – YOKOGAWA PROSAFE-RS
- 46 – SCHNEIDER ELECTRIC FOXBORO FCP280 / FCP270

- 47 – HONEYWELL CONTROLEDGE 900 series
- 48 – HONEYWELL EXPERION C300
- 49 – SCHNEIDER ELECTRIC MICOM C264
- 50 – UMAS device
- 51 – TASE.2 server
- 52 – PROFINET device
- 53 – DIRECTLOGIC
- 54 – Server with encryption support
- 55 – BACNET device
- 56 – SCHNEIDER ELECTRIC P545
- 57 – YCU/ELC
- 58 – FEU device
- 59 – Generic IED
- 60 – Generic Gateway
- 61 – Generic PLC
- 62 – VALMET DNA device
- 63 – IPU device
- 64 – OWEN PLC100 series
- 65 – CODESYS V2 based device
- 66 – PNU20 device
- 67 – KNX device
- 68 – DTS device
- 69 – B&R
- 70 – SIEMENS SICAM PAS server
- 71 – TELNET server
- 72 – VNIIA device
- 73 – CHINT MAS400

- 74 – CHINT MAS9600
- 75 – ISaGRAF device

- `Connection` – connection ID from the connections.csv file containing a description of connections.

The header strings are followed by the file body containing the values of parameters (device name, device class code, connection ID).

Example devices.csv file

```
'Devices
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Device;Type;Connection
"ms_plc";4;"ms_plc"
"mc_SysQ";8;"mc_SysQ"
```

Connections description file: connections.csv

A connections description file contains the IDs of connections, codes of application-layer protocols, and full network addresses of devices.

The file should begin with header strings containing the data needed for file processing.

Example header strings of the connections.csv file

```
'Connections
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;Protocol;Address
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;Protocol;Address` contains the names of columns with data:

- `Connection` – connection ID for description files.

  Connection ID is used to link protocols to devices and tags.

- `Protocol` – code of the application-level protocol. The following protocol codes are used:
  - 0 – MODBUS TCP
  - 1 – SIEMENS S7COMM over TCP
  - 2 – SIEMENS S7COMM over INDUSTRIAL ETHERNET
  - 3 – MITSUBISHI MELSEC SYSTEM Q
  - 4 – ALLEN-BRADLEY ETHERNET/IP
  - 5 – IEC 61850 MMS
  - 6 – IEC 61850 GOOSE
  - 7 – IEC 60870-5-104

- 8 – GENERAL ELECTRIC SRTP
- 9 – IEC 61850 SAMPLED VALUES
- 10 – SIEMENS S7COMMPLUS over TCP
- 11 – EMERSON DELTAV
- 12 – OMRON FINS over UDP
- 13 – MMS for ABB AC 800M
- 14 – YOKOGAWA VNET/IP
- 15 – CODESYS V3 GATEWAY over TCP
- 16 – DNP3
- 17 – OMRON FINS over TCP
- 18 – OPC UA BINARY
- 19 – DMS for ABB AC 700F
- 20 – OPC DA
- 21 – OMRON FINS over ETHERNET/IP
- 22 – CODESYS V3 GATEWAY over UDP
- 23 – BECKHOFF ADS/AMS
- 24 – IEC 60870-5-101
- 25 – FOXBORO FCP280 / FCP270 INTERACTION
- 26 – BSAP
- 27 – HONEYWELL CONTROLEDGE 900 INTERACTION
- 28 – WMI INTERACTION
- 29 – HONEYWELL EXPERION INTERACTION
- 30 – MiCOM C264 INTERACTION
- 31 – SCHNEIDER ELECTRIC UMAS
- 32 – TASE.2
- 33 – PROFINET IO
- 34 – DIRECTLOGIC INTERACTION
- 35 – BACNET

- 36 – YARD
- 37 – COS
- 38 – IPU-FEU INTERACTION
- 39 – VALMET DNA INTERACTION
- 40 – CODESYS V2
- 41 – PNU20
- 42 – GENERAL ELECTRIC EGD
- 43 – KNXnet/IP
- 44 – DTS
- 45 – INA2000
- 46 – SIEMENS SICAM SCC - INTERACTION with SICAM PAS
- 47 – TELNET
- 48 – VNIIA
- 49 – CHINT MAS400
- 50 – CHINT MAS9600
- 51 – ISaGRAF IXL
- 52 – ISaGRAF SNCP

- `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=192.168.2.7;Port=502"`

  Connection with the Mitsubishi System Q controller (one IP address, two ports):
  ```
  "Station1";3;"IP-Address=192.168.2.8;Port=5001 Network=0;Station=0;PC=255"
  "Station1";3;"IP-Address=192.168.2.8;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$Program";1;"IP-Address=192.168.2.21;Port=102;Rack=0;Slot=2"
  "S7$Program";1;"IP-Address=192.168.2.22;Port=102;Rack=0;Slot=2"
  ```

  The connection with the Siemens S7-400 controller uses two protocols: S7Comm over the TCP/IP stack, and S7Comm over the Industrial Ethernet network (one set of tags):
  ```
  "S7$Program";1;"IP-Address=192.168.2.21;Port=102;Rack=0;Slot=2"
  "S7$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).

Example connections.csv file

```
'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=192.168.2.77;Port=1025"
"mc_SysQ";7;"IP-Address=192.168.2.77;Port=2404;Asdu=555"
```

The format of the device network address in the file connections.csv depends on the type of protocol used.

Example:
The following address formats can be used for protocols supported by Kaspersky Industrial CyberSecurity for Networks:

- MODBUS TCP:
  `"IP-Address=192.168.2.7;Port=502"`
- SIEMENS S7COMM over TCP:
  `"IP-Address=192.168.2.7;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=192.168.2.7;Port=502;Network=0;Station=0;PC=255"`
- ALLEN-BRADLEY ETHERNET/IP:
  `"IP-Address=192.168.2.7;Port=44818"`
- IEC 61850 MMS:
  `"IP-Address=192.168.2.7;Port=502;Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 61850 GOOSE:
  `"Domains=IED_0009CTRL,IED_0009PROT;Vendor=SIEMENS;Model=Siprotec-6MD66x"`
- IEC 60870-5-104:
  `"IP-Address=192.168.2.7;Port=104;Asdu=2"`
- GENERAL ELECTRIC SRTP:
  `"IP-Address=192.168.2.50;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=192.168.2.22;Port=102"`
- EMERSON DELTAV:
  `"IP-Address=192.168.2.38;Port=18507"`
- OMRON FINS over UDP:
  `"IP-Address=192.168.2.1;Port=9600"`
- MMS for ABB AC 800M:
  `"IP-Address=192.168.2.60;Port=102"`
- YOKOGAWA VNET/IP:
  `"IP-Address=192.168.2.4;Port=5313"`

- CODESYS V3 GATEWAY over TCP:
  `"IP-Address=192.168.2.4;Port=11740"`
- DNP3:
  `"IP-Address=192.168.2.10;Port=20000"`
- OMRON FINS over TCP:
  `"IP-Address=192.168.2.1;Port=9600"`
- OPC UA BINARY:
  `"IP-Address=192.168.2.213;Port=49320"`
- DMS for ABB AC 700F:
  `"IP-Address=192.168.2.7;Port=9991"`
- OMRON FINS over ETHERNET/IP:
  `"IP-Address=192.168.2.1;Port=44818"`
- OPC DA:
  `"IP-Address=192.168.2.7;Port=135"`
- WMI INTERACTION:
  `"IP-Address=192.168.2.7;Port=135"`
- CODESYS V3 GATEWAY over UDP:
  `"IP-Address=192.168.2.7;Port=1740"`
- BECKHOFF ADS/AMS:
  `"IP-Address=192.168.2.7;Port=48898"`
- IEC 60870-5-101:
  `"IP-Address=192.168.2.7;Port=950"`
- FOXBORO FCP270, FCP280 INTERACTION:
  `"MAC=00:01:02:03:04:05"`
- BSAP:
  `"IP-Address=192.168.2.7;Port=1234"`
- HONEYWELL CONTROLEDGE 900 INTERACTION:
  `"IP-Address=192.168.2.99;Port=41103"`
- HONEYWELL EXPERION INTERACTION:
  `"IP-Address=192.168.2.10;Port=55553"`
- SCHNEIDER ELECTRIC UMAS:
  `"IP-Address=192.168.2.7;Port=502"`

- TASE.2:
  `"IP-Address=192.168.2.20;Port=102"`
- PROFINET IO:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.20\;Frame=IDS_TEL352"`
- DIRECTLOGIC INTERACTION:
  `"IP-Address=192.168.2.70;Port=28784"`
- BACNET:
  `"IP-Address=192.168.2.200;Port=47808"`
- YARD:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.1\;Port=2002"`
- COS:
  `"MAC=00:01:02:03:04:05\;IP-Address=192.168.2.131\;Port=3077"`
- IPU-FEU INTERACTION:
  `"IP-Address=192.168.2.200;Port=57005"`
- VALMET DNA INTERACTION:
  `"IP-Address=192.168.2.11;Port=2519"`
- CODESYS V2:
  `"IP-Address=192.168.2.200;Port=1210"`
- PNU20:
  `"IP-Address=192.168.2.200;Port=43962"`
- GENERAL ELECTRIC EGD:
  `"IP-Address=192.168.2.51;Port=18246"`
- KNXnet/IP:
  `"IP-Address=192.168.2.76;Port=3671"`
- DTS:
  `"IP-Address=192.168.2.11;Port=30000"`
- INA2000:
  `"IP-Address=192.168.2.1;Port=11159"`
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS:
  `"IP-Address=192.168.2.1;Port=10501"`
- TELNET:
  `"IP-Address=192.168.2.250;Port=23"`

- VNIIA:
  `"MAC=00:01:02:03:04:05"`
- CHINT MAS400:
  `"IP-Address=192.168.2.50;Port=46286"`
- CHINT MAS9600:
  `"IP-Address=192.168.2.50;Port=46286"`
- ISaGRAF IXL:
  `"IP-Address=192.168.2.50;Port=1131"`
- ISaGRAF SNCP:
  `"IP-Address=192.168.2.50;Port=1132"`

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.

Example header strings of the variables.csv file

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;E` contains the names of columns with data:

- `Id` – unique numerical ID of the tag.

  The tag ID is needed to create links to the tag in the datasets.csv file.

- `Varname` – full name of the tag (for example, `Drain.8450PT00058.value20`).

- `Connection` – ID of the connection with which the tag is linked.

  Connection ID is specified in the connections description file and is used for linking protocols to tags.

- `Address` – address of the tag in string form.

  The address depends on the type of the protocol with which the tag is linked (for example, for the S7comm protocol the address value is `M2.7`, `DB575:82.0`, and for the Modbus TCP protocol the address value is `400537`, `123`, `300001`).

- `Datatype` – numerical code of the tag data type. The following codes are used:
  - 0 – BOOL
  - 1 – INT8
  - 2 – UINT8
  - 3 – INT16
  - 4 – UINT16
  - 5 – INT32
  - 6 – UINT32
  - 7 – INT64
  - 8 – UINT64
  - 9 – FLOAT
  - 10 – DOUBLE
  - 11 – STRING
  - 12 – ENUM
  - 13 – BOOL ARRAY
  - 14 – UNSPECIFIED
- `Length` – string length in bytes for a tag of the string type.
- `InLo;InHi;OutLo;OutHi` – parameters for scaling the tag value.

  If the values of all parameters for scaling the tag value are equal to zero, scaling of the tag value is not used. If numerical values of parameters are specified, the following formula is used to calculate the tag value: TagValue = OutLo + (TagValue – InLo) * (OutHi – OutLo) / (InHi – InLo), where TagValue is the tag value.
- `Description` – tag description (for example, "Steam pressure at the output of Boiler No. 1").
- `EngUnits` – units of measurement of the physical quantity corresponding to the tag (for example, m/s, J).
- `EnumName` – name of the enumeration from the enums.csv file, which defines the value of the tag.

  The `EnumName` field can be filled for tags with data types ENUM, INT*, or UINT*. The `EnumName` field contains a link to the enumeration from the enums.csv file.

  Example 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).

Example variables.csv file

```
'Variables
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'ID;Varname;Connection;Address;Datatype;Length;InLo;InHi;OutLo;OutHi;Description;EngUnits;EnumName
5;"System.mitsub_n.ms_plc.Bit01";"ms_plc";"W0";4;0;0;0;0;0;"System.mitsub_n.ms_plc.Bit01";"";""
6;"System.mitsub_n.ms_plc.Register01";"ms_plc";"W20";9;0;0;0;0;0;"System.mitsub_n.ms_plc.Register01";"";""
1;"systemQ.Bit01";"mc_SysQ";"10";0;0;0;0;0;0;"systemQ.Bit01";"";""
```

The structure of the tag address in the `Address` field depends on the protocol used.

The following structure addresses are used for the supported protocols:

- MODBUS TCP: integer (for example, addresses of discrete inputs: from 100001).
- SIEMENS S7COMM over TCP and S7COMM over INDUSTRIAL ETHERNET: string in the format `[Area][ByteAddress].[BitAddress]`.

  If the condition `MemArea=DataBlocks` is satisfied, the address is supplemented with the number of the data block. The string changes to `[DB17]:[ByteAddress].[BitAddress]`, where:

  - `Area` – the enumeration of codes of memory areas according to the protocol standard: M, I, O, DB, C, T.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- MITSUBISHI MELSEC SYSTEM Q: a string in the format `[Area][Address]`, where:
  - `Area` – the enumeration of codes of memory areas according to the protocol specification: SM, SD, M, L, F, V, D, TS, TC, TN, SS, SC, SN, CS, CC, CN, S, Z, R, X, Y, B, W, SB, SW, DX, DY, ZR.
  - `Address` – the address value. The address is an integer in the range that depends on the data area.
- ALLEN-BRADLEY ETHERNET/IP: a string with the tag name.
- IEC 61850 MMS and GOOSE: per the IEC 61850 standard – a string of the format `DOMAIN=Domain;LN=LnName;CO=CoName;DA=FullTagName;CDC=CdcName;LNCDC=LNClassName`, where:
  - `DOMAIN` – a parameter that includes the device name and the logical device name.
  - `LN` – logical node name.
  - `CO` – functional constraint name.
  - `DA` – tag name.
  - `CDC` – attribute common data class name.
  - `LNCDC` – logical node common data class name.

- IEC 60870-5-104 and IEC 60870-5-101: a string in the format `[ASDU]:[Address]`, where:
  - `ASDU` – ASDU number represented by an integer.
  - `Address` – InformationObject number represented by an integer.
- GENERAL ELECTRIC SRTP: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` – the enumeration of codes of memory areas according to the protocol standard: I, Q, T, M, G, AI, AQ, R, P, L, W.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- SIEMENS S7COMMPLUS over TCP: string in the format `LID=LidValue;RID=RidValue`, where `LidValue` and `RidValue` are internal identifiers of a tag in the TiaPortal project.
- EMERSON DELTAV: a string with the tag name.
- OMRON FINS over UDP, OMRON FINS over TCP and OMRON FINS over ETHERNET/IP: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` – enumeration of codes of memory areas according to the protocol standard: A, CIO, C, CS, D, DR, E, H, IR, TK, T, TS, W.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- YOKOGAWA VNET/IP: a string with the tag name.
- DNP3: string in the format `[GROUP]:[INDEX]`, where:
  - `GROUP` is the specific group.
  - `INDEX` is the specific index.
- DMS for ABB AC 700F: integer.
- MMS for ABB AC 800M: string in the format `[Application]:[POUInstance].[VarOffset]`, where:
  - `Application` is the name of the application.
  - `POUInstance` is the POU instance.
  - `VarOffset` is the variable offset.
- CODESYS V3 GATEWAY over TCP and CODESYS V3 GATEWAY over UDP: string with the tag name.
- OPC UA BINARY: a string with the tag name.
- OPC DA: a string with the tag name.

- BSAP: string in the format `[MSD_VERSION]:[MSD]`, where:
  - `MSD_VERSION` is an integer in the range of 0–65535 that is used for comparing versions of projects/tags in the PLC and SCADA system.
  - `MSD` is the tag ID represented by an integer in the range of 0–65535.
- FOXBORO FCP280 / FCP270 INTERACTION: string containing the tag name.
- HONEYWELL EXPERION INTERACTION: string in the format `[EEC_ID]:[IOC_ID]:[DOC_ID]:[PC_ID]`, where:
  - `EEC_ID` is the ID of the runtime environment in the PLC program (Execution environment code) represented by an integer in the range of 0–65535.
  - `IOC_ID` is the ID of the I/O module in the PLC program (Input and output code) represented by an integer in the range of 0–65535.
  - `DOC_ID` is the ID of the subblock in the PLC program (Dependent object code) represented by an integer in the range of 0–65535.
  - `PC_ID` is the ID of the block parameter in the PLC program (Property code) represented by an integer in the range of 0–65535.
- DIRECTLOGIC INTERACTION: string in the format `[Area][ByteAddress].[BitAddress]`, where:
  - `Area` is the enumeration of memory area codes according to the protocol specification: X, Y, C, S, T, CT, GX, GY, V, P, SP, B, PB.
  - `ByteAddress` – the byte address represented by an integer.
  - `BitAddress` – the bit address inside the byte, which is represented by an integer.
- BACNET: string in the format `[OBJECT_TYPE]:[OBJECT_ID]`, where:
  - `OBJECT_TYPE` is the type of object according to the protocol specification.
  - `OBJECT_ID` is the sequence number of the object represented by an integer in the range of 0–4194303.
- PROFINET IO: string in the format `[IO]:[SubSlot]:[Index]:[Offset].[BitAddress]`, where:
  - `IO` is the variable direction (input, output).
  - `SubSlot` is the number of the subslot represented by an integer.
  - `Index` is the tag index represented by an integer.
  - `Offset` is the tag byte address represented by an integer.
  - `BitAddress` is the bit address inside the byte, which is represented by an integer (used only for tags that have the bool data type).

  In addition, to correctly load the protocol parameters, you must specify the GSDML file for the specific device.

- YARD: string in the format `[Controller Address]:[Index]:[Size]:[Config]:[MessageType]`, where:
  - `Controller Address` – address of the object controller represented by a hexadecimal integer.
  - `Index` – bit tag index represented by an integer.
  - `Size` – bit size represented by an integer.
  - `Config` – position of the jumpers on the object controller represented by a hexadecimal integer.
  - `MessageType` – type of message (`Order` or `Status`).

  In addition, to correctly load the protocol parameters, you may need to specify the configuration files for the specific device.
- COS: string in the format `[Object ID]:[Variable ID]`, where:
  - `Object ID` – object identifier represented by an integer.
  - `Variable ID` – variable identifier represented by an integer.

  In addition, to correctly load the protocol parameters, you must specify the configuration file for the station. The file name must be "specific.zip".
- VALMET DNA INTERACTION: string containing the tag name.

  In addition, to correctly load the protocol parameters, you must specify the file containing the PLC boot journal. The file name must be "specific.zip".
- PNU20: integer in the range of 0–65535.
- GENERAL ELECTRIC EGD: string in the format `[ExchangeId]:[RefAddress]`, where:
  - `ExchangeId` – subscription ID represented by an integer in the range of 0–4294967295.
  - `RefAddress` – tag address offset (in bytes) represented by an integer in the range of 0–65535.
- KNXnet/IP: integer in the range of 0–65535.
- SIEMENS SICAM SCC - INTERACTION with SICAM PAS: integer in the range 0–65535.
- CHINT MAS400: integer in the range 0–4294967295.
- CHINT MAS9600: integer in the range 0-4294967295.
- ISaGRAF IXL: positive integer.
- ISaGRAF SNCP: positive integer.

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.

Example header strings of the enums.csv file

```
'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).

Example enums.csv file

```
'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.

Example header strings of the datasets.csv file

```
'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).

Example datasets.csv file

```
'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.

Example header strings of the iec61850_mms_reports.csv file

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

The first three header strings are identical to the header strings in the devices.csv file.

The string `Connection;ReportName;ReportId;DataSetName;IsBuffered` contains the names of columns with data:

- `Connection` – ID of the connection associated with the string of settings in the file iec61850_mms_reports.csv.
- `ReportName` – name of the report.
- `ReportId` – ID of the report.
- `DataSetName` – name of the data set associated with this report.
- `IsBuffered` – indicates whether or not the report is buffered. It takes the `Buffered` or `Unbuffered` value.

The header strings are followed by the file body containing the parameter values (connection ID, report name, report ID, name of the data set for the report, and the buffer indicator).

Example iec61850_mms_reports.csv file

```
'Reports
'Format Version V1.0.0.0;KICS Importer Version V1.0.0.0
'Field separator: ; Decimal separator: . Text quotes: " Var name separator: .
'Connection;ReportName;ReportId;DataSetName;IsBuffered
```

```
"IED24151LD";"IED24151LD/LLN0$BR$brcbST01";"brcbST01";"IED24151LD/LLN0$DSList";"Buffered"
"IED24151LD";"IED24151LD/LLN0$RP$urcbMX01";"urcbMX01";"IED24151LD/LLN0$MXList";"Unbuffered"
```

System event types in Kaspersky Industrial CyberSecurity for Networks

In Kaspersky Industrial CyberSecurity for Networks, events are registered by using the system event types that are automatically created during installation of the application.

Each event type corresponds to a specific event registration technology.

System event types based on Deep Packet Inspection technology

This article provides a description of system event types associated with Deep Packet Inspection technology (see the table below).

System event types based on Deep Packet Inspection technology (DPI)

Code	Title of event type	Registration conditions
4000002900	$technology_rule	Process Control rule was triggered. The following variables are used in the title and description of a system event type: • $technology_rule – name of the rule. • $tags – received values of tags whose conditions are defined in the rule. The user-defined settings specified in the triggered Process Control rule are used for the title, description, and scoring of a registered event.
4000000001	Test event (DPI)	A test network packet was detected.

System event types based on Command Control technology

This article provides a description of a system event type associated with Command Control technology (see the table below).

System event type based on Command Control technology (CC)

Code	Title of event type	Registration conditions
4000002602	$systemCommandShort	A monitored system command was detected (and there is no enabled Interaction Control rule for the system command). The following variables are used in the title and description of an event type: • $systemCommandShort – brief description of the detected system command. • $systemCommandFull – detailed description of the detected system command. • $attackTechniques – list of possible techniques from the MITRE ATT&CK Knowledge Base that could be employed by cybercriminals for attacks using this system command.

System event types based on Asset Management technology

This article provides a description of system event types associated with Asset Management technology (see the table below).

System event types based on Asset Management technology (AM)

Code	Title of event type	Registration conditions
4000005003	Detected new device with the address $owner_ip_or_mac	Asset Management monitoring mode resulted in the automatic addition of a new device based on a detected IP address or MAC address that has not been specified for other devices in the table. When registering the event, the application may simultaneously register the risk named **Unauthorized device** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name – assigned name of the device. • $assigned_mac: the assigned MAC address (if defined) • $owner_ip: the assigned IP address (if defined) • $asset_id – ID of the device.
4000005004	Received new information about device with the address $owner_ip_or_mac	Asset Management monitoring mode resulted in the automatic update of device information based on data obtained from traffic. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name – name of the device. • $updated_params: a list of updated information • $asset_id – ID of the device.
4000005005	IP address $owner_ip conflict detected	In Asset Management monitoring mode, the application detected the use of an IP address by a different device than the device for which this IP address was specified. The following variables are used in the title and description of an event type: • $owner_ip: the IP address • $challenger_asset_name: the name of the device that used the IP address • $challenger_mac: the MAC address of the device that used the IP address • $asset_name: the name of the device in whose settings the IP address was specified • $owner_mac: the MAC address of the device in whose settings the IP address was specified • $challenger_ips_list: a list of other IP addresses of the device that used the IP address • $asset_id: the ID of the device in whose settings the IP address was specified • $challenger_id: the ID of the device that used the IP address
4000005006	Detected traffic from address $owner_ip_or_mac, which is assigned to a device with the Archived status	In Asset Management monitoring mode or based on data received from an EPP application, activity was detected from a device that was assigned a status of *Archived*. When registering the event, the application may simultaneously register the risk named **Unauthorized device** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name – name of the device. • $last_seen_timestamp: the date and time when the device was last seen in the network • $asset_id – ID of the device.
4000005007	A new IP address $new_ip_addr was detected for the device with MAC address $owner_mac	In Asset Management monitoring mode, a new IP address used by a device was detected. The following variables are used in the title and description of an event type: • $new_ip_addr: the detected IP address • $owner_mac: the MAC address of the device • $asset_name – name of the device. • $owner_ips_list: a list of other IP addresses of the device • $asset_id – ID of the device.

Code	Title of event type	Registration conditions
4000005008	MAC address $owner_mac was added to the device with IP address $owner_ip	Asset Management monitoring mode resulted in the automatic addition of a MAC address for a network interface for which only an IP address was specified (the device had a status of *Unauthorized* or *Archived*). The following variables are used in the title and description of an event type: • $owner_mac: the detected MAC address of the device • $owner_ip: the IP address of the device • $asset_name – name of the device. • $asset_id – ID of the device.
4000005009	IP address $owner_ip was added to the device with MAC address $owner_mac	Asset Management monitoring mode resulted in the automatic addition of an IP address for a network interface for which only a MAC address was specified (the device had a status of *Unauthorized* or *Archived*). The following variables are used in the title and description of an event type: • $owner_ip: the detected IP address of the device • $owner_mac: the MAC address of the device • $asset_name – name of the device. • $asset_id – ID of the device.
4000005010	Detected new MAC address $new_mac_addr for device with the IP address $owner_ip	In Asset Management monitoring mode, a new MAC address used by a device was detected. The following variables are used in the title and description of an event type: • $new_mac_addr: the detected MAC address • $owner_ip: the IP address of the device • $asset_name – name of the device. • $asset_id – ID of the device.
4000005011	Change of MAC address $owner_mac to $challenger_mac detected in device information received from EPP application	The MAC address of a device was updated according to data received from an EPP application. The following variables are used in the title and description of an event type: • $owner_mac: an old MAC address of the device • $challenger_mac: a new MAC address of the device • $asset_name – name of the device. • $asset_id – ID of the device.
4000005012	New address information for device $asset_name found in data received from EPP program	New address information of a device was detected in data received from an EPP application. This type of event is registered if a change in device address information was not processed by the application as an event with code 4000005009 or 4000005010. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $detected_epp_addresses: address information • $asset_id – ID of the device.
4000005013	Conflict detected in addresses of devices $conflicted_epp_assets after data received from EPP program	Based on data received from an EPP application, a conflict was detected in the addresses of multiple devices in Kaspersky Industrial CyberSecurity for Networks. According to data from the EPP application, the addresses belong to the same device. The following variables are used in the title and description of an event type: • $conflicted_epp_assets: devices with conflicting addresses detected • $unaccepted_epp_addresses – addresses that belong to the same device.
4000005014	Subnet $subnet_mask added based on data from EPP application	After data was received from an EPP application, a new subnet was automatically added to the list of known subnets. The subnet is added to an address space in which the data source may be the integration server that received data from an EPP application. If there are several of these address spaces available, the application chooses the address space that contains the most suitable subnet for automatically adding a new nested subnet. The following variables are used in the title and description of an event type: • $subnet_mask: a subnet address • $subnet_type: a subnet type
4000005015	Equipment change is detected for the device with the following address: $owner_ip_or_mac	Based on the data received from the EPP application, the device equipment information was updated using the equipment monitoring functionality. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name: a name of the device • $asset_id – ID of the device. • $added_asset_hardware: a list of added equipment • $modified_asset_hardware: a list of modified equipment • $removed_asset_hardware: a list of removed equipment

Code	Title of event type	Registration conditions
4000005200	PLC Project Control: detected read of unknown block from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of an unknown block of a project from a PLC (if there is no saved information about this block). When registering the event, the application may simultaneously register the risk named **Reading unknown block of project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name: the name of the block • $saved_date_time: the date and time when the operation was detected
4000005201	PLC Project Control: detected read of known block from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of a known block of a project from a PLC (if there is saved information about this block but the received information does not match the latest saved information about this block). When registering the event, the application may simultaneously register the risk named **Reading known block of project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name: the name of the block • $saved_date_time: the date and time when the block was saved in the application
4000005202	PLC Project Control: detected write of new block to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of an unknown block of a project from a PLC (if there is no saved information about this block). When registering the event, the application may simultaneously register the risk named **Writing new block of project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name: the name of the block • $saved_date_time: the date and time when the operation was detected
4000005203	PLC Project Control: detected write of known block to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a known block of a project from a PLC (if there is saved information about this block but the received information does not match the latest saved information about this block). When registering the event, the application may simultaneously register the risk named **Writing known block of project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $block_name: the name of the block • $saved_date_time: the date and time when the block was saved in the application
4000005204	PLC Project Control: detected read of unknown project from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of an unknown project from a PLC (if there is no saved information about this project). When registering the event, the application may simultaneously register the risk named **Reading unknown project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $saved_date_time: the date and time when the operation was detected
4000005205	PLC Project Control: detected read of known project from PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected read of a known project from a PLC (if there is saved information about this project but the received information does not match the latest saved information about this project). When registering the event, the application may simultaneously register the risk named **Reading known project from PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $saved_date_time: the date and time when the project was saved in the application

Code	Title of event type	Registration conditions
4000005206	PLC Project Control: detected write of new project to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a new project to a PLC (if there is no saved information about this project). When registering the event, the application may simultaneously register the risk named **Writing new project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $saved_date_time: the date and time when the operation was detected
4000005207	PLC Project Control: detected write of known project to PLC $asset_name	PLC Project Control read/write monitoring resulted in a detected write of a known project to a PLC (if there is saved information about this project but the received information does not match the latest saved information about this project). When registering the event, the application may simultaneously register the risk named **Writing known project to PLC** for this device. In this case, the risk is associated with the event. The following variables are used in the title and description of an event type: • $asset_name – name of the device. • $saved_date_time: the date and time when the project was saved in the application
4000005600	Changes detected in the list of users on the device with the address $owner_ip_or_mac	Changes to user information were detected while controlling users on devices. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name: a name of the device • $asset_id: the ID of the device • $added_asset_users: a list of added users • $modified_asset_users: a list of modified users • $removed_asset_users: a list of removed users
4000005601	Changes detected in the list of applications on the device with the address $owner_ip_or_mac	Changes to information about applications on the device were detected while monitoring applications and patches on devices. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name: a name of the device • $asset_id: the ID of the device • $added_asset_apps: a list of added applications • $removed_asset_apps: a list of removed applications
4000005602	Changes detected in the list of patches on the device with the address $owner_ip_or_mac	Changes in device patch information were detected while monitoring applications and patches on devices. The following variables are used in the title and description of an event type: • $owner_ip_or_mac: the IP or MAC address of the device • $asset_name: a name of the device • $asset_id: the ID of the device • $added_asset_patches: a list of added patches • $removed_asset_patches: a list of removed patches
4000005603	Changes detected in the configuration type $inventory_loc_key on the device	While monitoring device configurations, changes in the configuration type were detected when comparing to the previous configuration according to device scan results (for jobs that run in the **Update only** and/or **Archive versions** configuration processing modes). The following variables are used in the title and description of an event type: • $inventory_loc_key: the name of the configuration type • $device_config_inventory_changed_format: the changes detected in the configuration type
4000005604	Detected differences from the golden configuration $inventory_loc_key on the device	When monitoring device configurations, discrepancies were found compared to the golden configuration according to device scan results (for jobs that run in the **Compare to golden configuration** processing mode). The following variables are used in the title and description of an event type: • $inventory_loc_key: the name of the configuration type • $device_config_diverged_format: detected discrepancies compared to the golden configuration

Code	Title of event type	Registration conditions
4000005700	Detected public key mismatch when remotely connecting to device	While scanning or actively polling a device, a mismatch was detected between the received device public key and the value stored in the application. The program has canceled scanning or active polling of the device. The following variables are used in an event type description: • $asset_name: the name of the device • $new_asset_sshpublickey: received public key • $old_asset_sshpublickey: stored public key
4000000004	Test event (AM)	A test network packet was detected (with the device activity detection method enabled).

System event types based on Network Integrity Control technology

This article provides a description of system event types associated with Network Integrity Control technology (see the table below).

System event types based on Network Integrity Control technology (NIC)

Code	Title of event type	Registration conditions
4000002601	Unauthorized network interaction detected ($top_level_protocol)	A network interaction that is not specified in an enabled Interaction Control rule was detected. The following variables are used in the title and description of an event type: • $top_level_protocol – name of the top-level protocol. • $protocol – name of the application-level protocol.
4000002700	No traffic at monitoring point named $monitoringPoint	The network interface linked to the monitoring point has not received traffic in more than 15 seconds. The following variables are used in the title and description of an event type: • $monitoringPoint – name of the monitoring point. • $interface – name of the network interface that is linked to the monitoring point. • $duration – amount of time during which there was no traffic (in seconds).
4000000002	Test event (NIC)	A test network packet was detected (when Network Integrity Control is enabled).

System event types based on Intrusion Detection technology

This article provides a description of system event types associated with Intrusion Detection technology (see the table below).

System event types based on Intrusion Detection (IDS) technology

Code	Title of event type	Registration conditions
4000002701	TCP protocol anomaly detected: content substitution in overlapping TCP segments	TCP protocol anomaly detected: packets contain overlapping TCP segments with varying contents.
4000003000	Rule from the $fileName set (system set of rules) was triggered	Intrusion Detection rule from the system set of rules is triggered. The following variables are used in the title and description of an event type: • $fileName – name of the rule set. • $category – class of the rule. • $ruleName – name of the rule. • $signature_id – rule ID (sid).

Code	Title of event type	Registration conditions
4000003001	A rule from the $fileName set (user-defined rule set) was triggered.	Intrusion Detection rule from the user-defined rule set is triggered. The following variables are used in the title and description of an event type: • $fileName – name of the rule set. • $category – class of the rule. • $ruleName – name of the rule. • $signature_id – rule ID (sid). • $action – type of action to take on network packets defined in the rule (the `drop` or `reject` actions are not performed in Kaspersky Industrial CyberSecurity for Networks).
4000003002	Signs of a brute-force attack or scan were detected	A rule for detecting a scan or brute-force attack was triggered. In the event type description, the $ruleName variable is used for the rule name.
4000003003	Network Anomaly Detection rule was triggered	Network Anomaly Detection rule was triggered. When an event is registered, the event receives a title, score and description from the Network Anomaly Detection rule.
4000004001	Symptoms of ARP spoofing detected in ARP replies	Signs of falsified addresses in ARP packets detected: multiple ARP replies that are not associated with ARP requests. The following variables are used in an event type description: • $senderIp – substituted IP address. • $targetIp – IP address of the target node. • $attackStartTimestamp – time when the first ARP reply was detected.
4000004002	Symptoms of ARP spoofing detected in ARP requests	Signs of falsified addresses in ARP packets detected: multiple ARP requests from the same MAC address to different destinations. The following variables are used in an event type description: • $senderIp – substituted IP address. • $targetIp – IP address of the target node. • $attackStartTimestamp – time when the first ARP reply was detected.
4000005100	IP protocol anomaly detected: data conflict when assembling IP packet	IP protocol anomaly detected: data does not match when overlaying fragments of an IP packet.
4000005101	IP protocol anomaly detected: fragmented IP packet size exceeded	An IP protocol anomaly was detected: the actual total size of a fragmented IP packet after assembly exceeds the acceptable limit.
4000005102	IP protocol anomaly detected: the size of the initial fragment of the IP packet is less than expected	An IP protocol anomaly was detected: the size of the initial fragment of an IP packet is less than the minimum permissible value.
4000005103	IP protocol anomaly detected: mis-associated fragments	An IP protocol anomaly was detected: fragments of an assembled IP packet contain conflicting data on the length of the fragmented packet.
4000000003	Test event (IDS)	A test network packet was detected (with rule-based Intrusion Detection enabled).

System event types based on External technology

This article provides a description of system event types associated with External technology (see the table below).

System event types based on External technology (EXT)

Code	Title of event type	Registration conditions
8000000001	Incident	A sequence of events satisfying the conditions of a correlation rule was detected. When an event is registered, the incident receives a title and description from the correlation rule.
4000005400	Event from an external system	An event was received from an external system using the Kaspersky Industrial CyberSecurity for Networks API. When an event is registered, the contents of the title and description are determined by the external system.

System event types based on Endpoint Protection Platform

This article provides a description of system event types associated with Endpoint Protection Platform technology (see the table below).

System event type based on Endpoint Protection Platform (EPP)

Code	Title of event type	Registration conditions
4000005500	Activity specific for network attacks	The integration server received data indicating that the Network Threat Protection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005501	Connection of an untrusted external device	The integration server received data indicating that the Device Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005502	Attempt to run an unauthorized or untrusted application	The integration server received data indicating that the Application Launch Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005503	Prohibited file operation in the specified monitoring scope	The integration server received data indicating that the File Integrity Monitor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005504	Files in the specified monitoring scope are modified	The integration server received data indicating that the Baseline File Integrity Monitor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005505	Network connection not allowed by firewall rules	The integration server received data indicating that the Firewall Management component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005506	System registry modifications in the specified monitoring scope	The integration server received data indicating that the Registry Access Monitor component of the EPP application is triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005507	Log analysis rule is triggered	The integration server received data indicating that a rule of the Log Inspection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005508	Attempt to exploit a vulnerability in a protected process	The integration server received data indicating that the Exploit Prevention component of the EPP application is triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005509	Attempt to maliciously encrypt network file resources	The integration server received data indicating that the Anti-Cryptor component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005510	Attempt to connect to a Wi-Fi network	The integration server received data indicating that the Wi-Fi Control component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005511	PLC project was modified compared to the baseline	The integration server received data indicating that the PLC Project Integrity Check component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.

Code	Title of event type	Registration conditions
4000005512	Infected or probably infected object is detected	The integration server received data indicating that the Real-Time File Protection component of the EPP application was triggered. The event type description uses the variable $epp_event_description for data from the EPP application.
4000005513	Sigma rule $sigmaAlertTitle triggered	The integration server received data about an Endpoint Agent component Sigma rule being triggered. The following variables are used in the title and description of an event type: • $sigmaAlertTitle: Sigma rule name • $sigma_detection_type: detection technology • $sigma_object_type: the type of object that triggered the Sigma rule • $sigma_object_name: the name of object that triggered the Sigma rule or the name of the first triggered Sigma rule • $sigma_status: detection status

Categories of system commands in Kaspersky Industrial CyberSecurity for Networks

This article lists the categories of system commands supported by Kaspersky Industrial CyberSecurity for Networks when analyzing industrial network traffic (see the table below).

Categories of system commands

Category of system commands	Description
`Connection`	Connection management commands.
`Authentication`	Authentication commands.
`Operating mode changes`	Commands for changing the operating mode of devices.
`Download program`	Commands for downloading a program of devices.
`Upload program`	Commands for uploading a program of devices.
`Control commands`	Standardized commands for protocols of intelligent electronic devices (IED).
`Modify program`	Commands for changing the control program of a device.
`Alarm signal management`	Commands for managing alarm signals.
`Live mode`	Commands for working with a program of devices in live or debug mode.
`Modify tags`	Commands for enforcing modifications to tag values.
`Reading tags and data`	Commands for receiving tag values, subscribing to tags, and requesting data on programs of devices.
`Update firmware`	Commands for modifying the firmware of devices.
`Read device configuration`	Commands for reading or requesting device information.
`Change device configuration`	Commands for modifying the settings of devices.
`File operation`	Commands for managing files and directories of devices.
`Service command`	Commands for servicing devices.
`Date and time management`	Commands for managing the date and time on devices.
`Diagnostic message`	Diagnostic messages regarding errors or mismatched data in traffic.
`Interaction via DCOM`	Commands of protocols that use DCOM technology (for example, OPC DA).
`Message parsing error`	Errors when parsing messages.
`Other`	Commands not assigned to other specific categories.

Examples of using address spaces in Kaspersky Industrial CyberSecurity for Networks

Address spaces (AS) enable operation of Kaspersky Industrial CyberSecurity for Networks in situations in which devices with identical addresses are used in different network segments. This article provides examples of using address spaces for the following options when duplicating device addresses in different network segments:

- Duplication of IP addresses
- Duplication of MAC addresses
- Duplication of MAC addresses and use of identical ranges of IP addresses

Address spaces for duplicating IP addresses of devices

This example examines a company that has 16 industrial sites with groups of PLCs at these sites. Each industrial site uses the same ranges of IP addresses: 10.4.0.0/16, 10.5.0.0/16, 10.8.0.0/16, 10.9.0.0/16. This means that devices at different sites may have identical IP addresses.

The network segments of industrial sites are completely isolated from the main enterprise network. Each segment contains operational PLCs, engineering workstations, and computers performing functions of application stations (hereinafter referred to as "Application Station" computers). A segment is integrated with the main enterprise network through an Application Station computer. This computer has a dedicated network interface with a unique IP address on the main enterprise network.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, the following objects must be added for each industrial site segment:

- Monitoring point for receiving traffic within the segment
- Monitoring point for receiving traffic from the Application Station computer
- Address space containing one rule

For example, you can add objects with the following names for the first segment:

- **MPoint_1-1**
- **MPoint_1-2**
- **Site_1**

The settings of address spaces for each segment are described in the table below.

AS for segments with identical IP addressing

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points**: MPoint_1-1 MPoint_1-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_2	**Monitoring points**: MPoint_2-1 MPoint_2-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
Site_3	**Monitoring points**: MPoint_3-1 MPoint_3-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16
...				
Site_16	**Monitoring points**: MPoint_16-1 MPoint_16-2	**Network (L3)**	**Any or not used**	10.4.0.0/16 10.5.0.0/16 10.8.0.0/16 10.9.0.0/16

Address spaces for duplicating MAC addresses of devices

This example examines an industrial network that uses VLAN technology. The network has two dedicated segments for industrial sites distinguished by the IDs VLAN 3910 and 3915. The network segments contain devices with manually assigned MAC addresses (the devices and their software support this capability). This means that devices in different network segments may have identical MAC addresses.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, an address space must be added for each segment. For example, the names **Site_1** and **Site_2** can be assigned to the address spaces. Address spaces may contain one rule each.

The settings of address spaces for each segment are described in the table below.

AS for segments with identical MAC addressing

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points**: **any**	**Data Link (L2)**	3910	**Any**
Site_2	**Monitoring points**: **any**	**Data Link (L2)**	3915	**Any**

Address spaces for duplicating MAC addresses of devices with the same range of IP addresses

This example examines an industrial network that uses VLAN technology. The network has two dedicated segments for industrial sites distinguished by the IDs VLAN 3910 and 3915. The network segments contain devices with manually assigned MAC addresses (the devices and their software support this capability). The IP addresses in each segment are in the same addresses range: 140.80.0.0/16. This means that devices in different network segments may have identical MAC addresses and/or identical IP addresses.

To ensure proper functioning of Kaspersky Industrial CyberSecurity for Networks in this configuration, an address space must be added for each segment. For example, the names **Site_1** and **Site_2** can be assigned to the address spaces. Address spaces may contain one rule each.

The settings of address spaces for each segment are described in the table below.

AS for segments with identical MAC addressing and identical IP address ranges

AS name	Data source	OSI model layers	VLAN ID	IP addresses
Site_1	**Monitoring points**: **any**	**Data Link and Network (L2 and L3)**	3910	140.80.0.0/16
Site_2	**Monitoring points**: **any**	**Data Link and Network (L2 and L3)**	3915	140.80.0.0/16

Supported common protocols

Kaspersky Industrial CyberSecurity for Networks supports traffic monitoring for 137 common protocols. The application monitors the following protocols:

1. AeroAdmin over TCP
2. AFP
3. Ammyy Admin over TCP
4. AnyDesk over TCP
5. ARP
6. Bitcoin over TCP
7. BitTorrent over TCP
8. BitTorrent over UDP
9. BOOTP / DHCP
10. Dameware MRC
11. DCE/RPC
12. DICOM over TCP
13. DNS
14. DNS/LLMNR over TCP
15. DNS/LLMNR over UDP
16. Dogecoin over TCP
17. Dropbox LAN Sync over UDP

18. EIGRP
19. Ethernet I
20. Ethernet II
21. Ether-S-IO over TCP
22. Ether-S-IO over UDP
23. Finger
24. Flash Media Server
25. FTP
26. FTP Data
27. GLBP over UDP
28. GRE
29. HiDiscovery
30. HL7 v2 over TCP
31. HL7 v3 over TCP
32. HSRP over UDP
33. HTTP
34. HTTP/2
35. HTTPS
36. IBM DB2
37. ICMP
38. Ident
39. IGMP
40. IMAP
41. IPv6
42. IPv6 Encapsulated
43. IPX
44. IRC
45. IS-IS over Ethernet I

46. IS-IS over Ethernet II
47. IS-IS over IPv4
48. ISO TSAP (ISO 8072)
49. Jabber XMPP over TCP
50. Kerberos over TCP
51. Kerberos over UDP
52. LDAP(S) over TCP
53. LDAP(S) over UDP
54. LDP
55. Link Layer Discovery Protocol (LLDP)
56. Litecoin over TCP
57. Loopback
58. mDNS over UDP
59. MikroTik Neighbor Discovery Protocol (MNDP)
60. MPLS
61. MPLS multicast
62. MQTT over TCP
63. MS SQL Server
64. MSNP over TCP
65. MSNP over UDP
66. MySQL
67. Napster
68. NBNS over UDP
69. NetBIOS
70. Network Time Protocol (NTP)
71. NFS over TCP
72. NFS over UDP
73. ONVIF over TCP

74. Open Shortest Path First (OSPF)
75. Oracle DB
76. PIM
77. POP3
78. PPTP
79. Precision Time Protocol (PTP)
80. PRP
81. QTP
82. RADIUS over UDP
83. RARP
84. RDP over TCP
85. RDP over UDP
86. Reliable Data Protocol
87. Remote Utilities over TCP
88. RIP
89. Rlogin
90. RSH
91. RTSP over TCP
92. SAIA S-Bus over TCP
93. SAIA S-Bus over UDP
94. SCTP
95. SFTP
96. SIP over UDP
97. SMB
98. SMB v2 over TCP
99. SMB v2 over UDP
100. SMB v3 over TCP
101. SMB v3 over UDP

102. SMB over UDP

103. SMTP

104. SNMP

105. SNMP v1 over UDP

106. SNMP v2 over UDP

107. SNMP v3 over UDP

108. SSDP

109. SSH

110. SSL v2

111. SSL v3

112. SSL/TLS

113. STP

114. SuiteLink over TCP

115. Syslog

116. Syslog over UDP

117. TCP

118. TeamViewer over TCP

119. TeamViewer over UDP

20. Telegram MTProto over TCP

121. Telnet

22. TFTP over TCP

23. TFTP over UDP

24. TLS v1.0

25. TLS v1.1

26. TLS v1.2

127. TLS v1.3

28. TNS over TCP

29. TNS over UDP

30. Tor over TCP

131. Tor over UDP

32. UDP

33. VNC

34. VRRP over IPv4

35. WebSocket

36. Cisco discovery protocol (CDP)

37. Radmin over TCP

Details on retrieving configurations for device types using configuration control jobs

When adding configuration control jobs, you can select the device types according to which the application will receive data during device scans.

This section contains information about the special features of receiving configurations for different types of devices.

Configurations of devices running Windows operating systems

You can get configurations for devices of the **Windows operating system** type that are running operating systems supported by Kaspersky Endpoint Agent for Kaspersky Industrial CyberSecurity for Networks integration scenarios.

For the **Windows operating system** type of devices, you can specify the following configuration types for receiving data:

- **Users**.
- **Groups**.
- **Applications**.
- **Patches**.
- **Services**.
- **Drivers**.
- **Scheduled tasks**.
- **Network shared resources**.

- **IP-to-network name consistency**.
- **IP-to-NetBIOS name consistency**.
- **Startup items**.
- **Password policies**.
- **Audit policies**.
- **Advanced audit policies**.
- **ARP table items**.
- **Routing table**.

Retrievable data on users

If the **Users** configuration type is specified for the configuration control job, the user account data on a device is read when the device is scanned. The application lets you receive the following data on each user account:

- Username in `domain\username` format.
- Unique ID of the user.
- Full name of the user (for example, `John Smith`).
- Indication of whether the user account is active.
- Indication of whether the user account is blocked.
- Indication of whether the user account password may expire.
- Indication of whether the password has expired.
- Indication of whether the user can change their password.
- List of groups that include the user.

Retrievable data on groups

If the **Groups** configuration type is specified for the configuration control job, the group account data on a device is read when the device is scanned. The application lets you receive the following data on each group account:

- Group name in the format `domain\group name`.
- Unique ID of the group.

- List of users included in the group. Each item in the list contains the following data:
  - Unique ID of the group member.
  - Name of the group member.

Retrievable data on applications

If the **Applications** configuration type is specified for the configuration control job, the data on installed applications on a device is read when the device is scanned. The application lets you receive the following data on each application:

- Application name.
- Application vendor.
- Size of the application in bytes.
- Application version.
- Date and time when the application was installed.

Retrievable data on patches

If the **Patches** configuration type is specified for the configuration control job, the data on installed patches for applications on a device is read when the device is scanned. The application lets you receive the following data on each patch:

- Patch name.
- Application vendor.
- Application for which the patch is installed.
- Patch version.

Retrievable data on services

If the **Services** configuration type is specified for the configuration control job, the data on registered services on a device is read when the device is scanned. The application lets you receive the following data on each service:

- Service name.
- Full name of the service.
- Startup type.

- Start command.
- Names of dependent services.

Retrievable data on drivers

If the **Drivers** configuration type is specified for the configuration control job, the data on installed drivers on a device is read when the device is scanned. The application lets you receive the following data on each driver:

- Driver name.
- Full name of the driver.
- Startup type.
- Path to the driver file.
- Names of dependent drivers.

Retrievable data on scheduled tasks

If the **Scheduled tasks** configuration type is specified for the configuration control job, the data on registered tasks in the Task Scheduler on a device is read when the device is scanned. The application lets you receive the following data on each task:

- Task name.
- Task status.
- Description.
- Creator.
- Commands executed when the task is started (actions related to running the executable code).

Retrievable data on shared network resources

If the **Network shared resources** configuration type is specified for the configuration control job, the data on created shared network resources on a device is read when the device is scanned. The application lets you receive the following data on each shared network resource:

- Network name of the shared resource.
- Local path to the network resource.
- Description.

- Type of network resource.
- Maximum number of connections.

Retrievable data from the IP-to-network name mapping table

If the **IP-to-network name consistency** configuration type is specified for the configuration control job, the data on items in the IP-to-network name mapping table (\etc\hosts) on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Network name.

Retrievable data from the IP-to-NetBIOS name mapping table

If the **IP-to-NetBIOS name consistency** configuration type is specified for the configuration control job, the data on items in the IP-to-NetBIOS name mapping table (\etc\lmhosts) on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Network name.
- Indication of whether the entry is loaded into the name cache.
- Specific domain of the entry.
- Lmhosts include files.

Retrievable data on startup items

If the **Startup items** configuration type is specified for the configuration control job, the data on operating system startup items on a device is read when the device is scanned. The application lets you receive the following data on each startup item:

- Information about the startup point (for example, the path in the system registry).
- Executable command or file (COM object).

Retrievable data on password policies

If the **Password policies** configuration type is specified for the configuration control job, a device's password policy data is read when the device is scanned. The application lets you receive the following data on each password policy:

- Maximum password age.
- Minimum password age.
- Minimum password length.
- Number of old passwords stored in history.
- Indication of whether the password must meet password complexity requirements.
- Indication of whether password encryption is reversible.

Retrievable data on audit policies

If the **Audit policies** configuration type is specified for the configuration control job, a device's audit policy data is read when the device is scanned. The application lets you receive the following data on each audit policy:

- Level of the account logon audit.
- Level of the account management audit.
- Audit level for access to objects in Active Directory Domain Services.
- Level of the logon audit.
- Audit level for access to objects that are not in Active Directory Domain Services.
- Audit level for policy change.
- Audit level for privilege use.
- Audit level for detailed tracking.
- Audit level for system events.

Retrievable data on advanced audit policies

If the **Advanced audit policies** configuration type is specified for the configuration control job, the device's advanced audit policy data is read when the device is scanned. The application lets you receive the following data on each advanced audit policy:

- Basic policy used to conduct the advanced audit.
- Subcategory of the basic policy.
- Audit level.

Retrievable data on ARP table items

If the **ARP table items** configuration type is specified for the configuration control job, the data on ARP table items on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Hardware address.
- Name of the network interface or adapter.
- Hardware address type.
- Entry type.

Retrievable data on the routing table

If the **Routing table** configuration type is specified for the configuration control job, the data on routing table items on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- Interface name or IP address.
- Destination subnet.
- Destination subnet mask.
- Gateway (address of the next router in the remote network).
- Protocol.

Configurations of devices running Linux operating systems

The **Linux operating system** type of devices is obtained on devices that use commands to run standard diagnostic utilities for Linux devices.

For the **Linux operating system** type of devices, you can specify the following configuration types for receiving data:

- **Users**.
- **Applications**.
- **ARP table items**.
- **IP-to-network name consistency**.
- **IP-to-NetBIOS name consistency**.
- **Scheduled tasks**.
- **Services**.
- **Routing table**.
- **Permissions of privileged groups and users**.

Retrievable data on users

If the **Users** configuration type is specified for the configuration control job, the user account data on a device is read when the device is scanned. The application lets you receive the following data on each user account:

- Username in `domain\username` format.
- Unique ID of the user.
- Full name of the user (for example, `John Smith`).
- Indication of whether the user account is active.
- Indication of whether the user account is blocked.
- Indication of whether the user account password may expire.
- Indication of whether the password has expired.
- Indication of whether the user can change their password.
- List of groups that include the user.

Retrievable data on applications

If the **Applications** configuration type is specified for the configuration control job, the data on installed applications on a device is read when the device is scanned. The application lets you receive the following data on each application:

- Application name.
- Size of the application in bytes.
- Application version.
- Date and time when the application was installed.

Retrievable data on ARP table items

If the **ARP table items** configuration type is specified for the configuration control job, the data on ARP table items on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Hardware address.
- Name of the network interface or adapter.
- Hardware address type.

Retrievable data from the IP-to-network name mapping table

If the **IP-to-network name consistency** configuration type is specified for the configuration control job, the data on items in the IP-to-network name mapping table (from the \etc\hosts file) on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Network name.

Retrievable data from the IP-to-NetBIOS name mapping table

If the **IP-to-NetBIOS name consistency** configuration type is specified for the configuration control job, the data on items in the IP-to-NetBIOS name mapping table (from the /etc/lmhosts file) on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- IP address.
- Network name.

Retrievable data on scheduled tasks

If the **Scheduled tasks** configuration type is specified for the configuration control job, the data on registered tasks in the Task Scheduler on a device is read when the device is scanned. The application lets you receive the following data on each task:

- Task name.
- Task status.
- Task start schedule.
- Creator.
- Executable command.

Retrievable data on services

If the **Services** configuration type is specified for the configuration control job, the data on services on a device is read when the device is scanned. The application lets you receive the following data on each service:

- Service name.
- Startup type.
- Start command.

Retrievable data on the routing table

If the **Routing table** configuration type is specified for the configuration control job, the data on routing table items on a device is read when the device is scanned. The application lets you receive the following data on each table item:

- Interface name or IP address.
- Destination subnet.
- Destination subnet mask.
- Gateway (address of the next router in the remote network).

Retrievable data on the permissions of privileged groups and users

If the **Permissions of privileged groups and users** configuration type is specified for the configuration control job, the data on privileged group and user permissions (from the \etc\sudoers file) on a device is read when the device is scanned. The application lets you receive the following data on the permissions of privileged groups and users:

- Full path to the \etc\sudoers file.
- Textual representation of the \etc\sudoers file or additional files included via the `include` and `includedir` directives.

Configurations of devices categorized as network equipment

The current version of the application lets you receive a configuration for the **Network devices** device type for the following devices:

- Cisco IOS™ devices.
- Eltex MES series.
- Hirschmann MACH and RS20 series.
- Moxa PT and EDS series.

  > Configuration retrieval capabilities for Moxa PT series devices are not supported when the device is in default setup mode (MENU mode).

- Siemens RUGGEDCOM® RSG2100 and SCALANCE series with SSH protocol support.
- D-Link® DES and DGS series (supported only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).
- MikroTik RouterOS devices (supported only in Kaspersky Industrial CyberSecurity for Networks version 4.5.1).

For the **Network devices** device type, you can specify the following configuration types for receiving data:

- **Users**.
- **ARP table items**.
- **Platform version**.
- **Executable processes**.
- **Startup configuration**.
- **Running configuration**.
- **Routing table**.
- **MAC table**.
- **Network interfaces**.

Retrievable data on Cisco IOS devices

The application retrieves the following data when scanning Cisco IOS devices:

- User data:
  - Username in `domain\username` format.
  - Unique ID of the user.
  - Indication of whether an SSH key is set up.
  - Indication of whether a password has been configured.
  - Indication of whether a secret has been configured for the user.
  - User privilege level.
- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
  - Entry type.
- OS version.

- Data on running processes:
  - Unique ID of the process.
  - Process name.
- Data on the startup configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the routing table:
  - Interface name or IP address.
  - Destination subnet.
  - Destination subnet mask.
  - Gateway (address of the next router in the remote network).
  - Protocol.
- Data on the MAC table:
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.
- Data on network interfaces:
  - Description.
  - Indication of whether the network interface is enabled.
  - MAC address.
  - Name.
  - Indication of whether the network interface is a physical interface.
  - Assigned IP address.

Retrievable data on Eltex MES series devices

The application retrieves the following data when scanning Eltex MES series devices:

- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
  - Entry type.
- OS version.
- Data on the startup configuration:
  - Name of the parameter section.
  - Textual representation of section parameters (output of the `show startup-config` command).
- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the routing table:
  - Interface name or IP address.
  - Destination subnet.
  - Destination subnet mask.
- Data on the MAC table:
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.
- Data on network interfaces:
  - Description.
  - Indication of whether the network interface is enabled.

- MAC address.
- Name.
- Indication of whether the network interface is a physical interface.

Retrievable data on Hirschmann RS20 and MACH series devices

The application retrieves the following data when scanning Hirschmann RS20 and MACH series devices:

- User data:
  - Username in `domain\username` format.
  - Operator access mode.
  - Authentication type.
  - Encryption type.
  - User access mode.
- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
- OS version.
- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the MAC table:
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.

Retrievable data on Moxa EDS and PT series devices

The application retrieves the following data when scanning Moxa EDS and PT series devices:

- OS version.
- Data on the startup configuration:
  - Name of the parameter section.
  - Textual representation of section parameters (output of the `show startup-config` command).
- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- MAC address table details (supported for Moxa EDS series devices only):
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.

Retrievable data on Siemens RUGGEDCOM RSG2100 and SCALANCE series devices with SSH protocol support

The application retrieves the following data when scanning Siemens RUGGEDCOM RSG2100 and SCALANCE series devices:

- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
  - Recording type (supported only for Siemens SCALANCE series devices).
- OS version.

- Data on the startup configuration:
  - Name of the parameter section.
  - Textual representation of section parameters (output of the `info` command at different nesting levels for Siemens SCALANCE series devices).
- Running configuration details (supported for Siemens RUGGEDCOM RSG2100 series devices only):
  - Name of the parameter section.
  - Textual representation of section parameters.
- MAC address table details (supported for Siemens RUGGEDCOM RSG2100 series devices only):
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.

Retrievable data on D-Link DES and DGS devices

The application retrieves the following data when scanning D-Link DES and DGS devices:

- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
  - Entry type.
- OS version.
- Data on the startup configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.

- Data on the routing table:
  - Interface name or IP address.
  - Destination subnet.
  - Destination subnet mask.
  - Gateway (address of the next router in the remote network).
  - Protocol.
- Data on the MAC table:
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.

Retrievable data on MikroTik RouterOS devices

The application retrieves the following data when scanning MikroTik RouterOS devices:

- User data:
  - User name.
  - User account description.
  - Indication of whether the user account is active.
- Data on ARP table items:
  - IP address.
  - Hardware address.
  - Name of the network interface or adapter.
  - Hardware address type.
  - Entry type.
- OS version.

- Data on the running configuration:
  - Name of the parameter section.
  - Textual representation of section parameters.
- Data on the routing table:
  - Interface name or IP address.
  - Destination subnet.
  - Destination subnet mask.
  - Gateway (address of the next router in the remote network).
- Data on the MAC table:
  - VLAN number.
  - MAC address.
  - Type of MAC address.
  - Port of MAC address.
- Data on network interfaces:
  - Indication of whether the network interface is enabled.
  - MAC address.
  - Name.

Configurations of PLCs and other devices received using Active poll connectors

The built-in **Active poll** connector type can receive a configuration for the **PLC** device type for the following devices:

- Emerson DeltaV
- Rockwell Automation Allen-Bradley
- Schneider Electric Modicon: M580, M340
- Siemens SIMATIC S7-300, S7-400
- Siemens SIMATIC S7-1200, S7-1500
- PLC based on the CODESYS V3 platform (for example, Prosoft-Systems Regul R500)

Retrievable data on Emerson DeltaV devices

When scanning Emerson DeltaV devices using **Active poll** connectors, the application lets you receive the following data:

- General settings:
  - Model or family of devices.
  - PLC device series.
  - PLC redundancy indicator.
- Settings for CPU modules and each received card:
  - Number of the slot containing the card (among all carriers).
  - CPU module vendor.
  - Type of module or card.
  - Module model (model of the CPU module or I/O card).
  - Brief description of the I/O card.
  - Unique alphanumeric part number, catalog number.
  - Hardware version.
  - Version of the IDE and firmware of controllers and cards.
  - Unique name of the controller defined by the user in the IDE.
  - Unique ID of the controller assigned in the IDE.
  - Serial number of the PLC CPU module.
- Settings for each received PLC project file:
  - Name of the project module (file).
  - Date when each of the configuration files was loaded into the PLC.
  - Checksum of the project module.

Retrievable data on Rockwell Automation Allen-Bradley devices

When scanning Rockwell Automation Allen-Bradley devices using **Active poll** connectors, the application lets you receive the following data:

- Settings for each received module:
  - Slot number in the rack containing the module.
  - Module vendor.
  - Module type.
  - Product (module) code.
  - Information about the module model.
  - Firmware version.
  - Unique name of the controller defined by the user in the IDE.
  - Serial number of the module.
  - Composite status of the module.
- General settings of the PLC project:
  - Slot number of the module assigned to the project.
  - User-defined name.
  - User-defined description.
- Settings for each program and routine of the PLC project:
  - Name of the project task.
  - Type of the project task.
  - Priority of the project task.
  - Name of the project program.
  - Name of the routine in the project program.
  - Checksum of the routine.

Retrievable data on Schneider Electric Modicon devices

When scanning Schneider Electric Modicon devices using **Active poll** connectors, the application lets you receive the following data:

- General settings:
  - PLC model or family.
  - Automation system development software used to configure the device.
  - Number of racks in the PLC installation.
- Settings for each received module:
  - Number of the rack containing the module.
  - Slot number in the rack containing the module.
  - CPU module vendor.
  - Module type.
  - Information about the module model.
  - Module firmware version.
  - Unique ID of the module.
  - Operating mode or status of the CPU module.
- General settings of the PLC project:
  - User-defined name.
  - Hash sum.
  - Name and version of the development environment (IDE) in which the project was last fully built.
  - Date and time of the last complete build of the project.
  - Name and version of the development environment (IDE) in which the last partial build of the project was performed (for individual project blocks).
  - Date and time of the last partial build of the project.
  - User-defined version of the project.
- Settings for each received PLC project block:
  - Type of Task setting assigned to the block.
  - User-defined name.

- Type of block and the language of the mnemonic diagrams in which the block is written.
- Checksum.

Retrievable data on Siemens SIMATIC devices of the S7-300 and S7-400 series

When scanning Siemens SIMATIC S7-300 and S7-400 series devices using **Active poll** connectors, the application lets you receive the following data:

- General settings:
  - PLC model or family.
  - Automation system development software used to configure the device.
  - Number of racks in the PLC installation.
  - Memory status.
  - Security settings.
- Settings for each received module:
  - Number of the rack containing the module.
  - Slot number in the rack containing the module.
  - CPU module vendor.
  - Module type.
  - Information about the module model.
  - Module ID according to the Siemens catalog.
  - Unique alphanumeric code of the Siemens module (MLFB).
  - Module hardware version.
  - Module firmware version.
  - Initial bootloader version.
  - Serial number of the CPU module.
  - Requested operating mode of the CPU module (the mode that should be enabled as a result of the transition).
  - Current operating mode of the CPU module.
- Hash sum of the PLC project.

- Settings for each received PLC project block:
  - Type.
  - ID.
  - Language of the mnemonic diagrams in which the block is written.
  - Checksum.
  - Compilation date.
  - Information about the creator or development environment.

Retrievable data on Siemens SIMATIC devices of the S7-1200 and S7-1500 series

When scanning Siemens SIMATIC S7-1200 and S7-1500 series devices using **Active poll** connectors, the application lets you receive the following data:

- General settings:
  - PLC model or family
  - Memory status.
  - Security settings.
- Settings for each received module:
  - Slot number in the rack containing the module.
  - CPU module vendor.
  - Module type.
  - Information about the module model.
  - Unique alphanumeric code of the Siemens module (MLFB).
  - Module firmware version.
  - Serial number of the CPU module.
  - Current operating mode of the CPU module.
- Hash sum of the PLC project.
- Settings for each received PLC project block:
  - Type.
  - ID.

- Language of the mnemonic diagrams in which the block is written.
- Checksum.
- Compilation date.

Retrievable data on a PLC based on the CODESYS V3 platform

When scanning a PLC based on the CODESYS V3 platform using **Active poll** connectors, the application lets you receive the following data:

- General settings:
  - PLC model.
  - PLC manufacturer.
  - Firmware version.
- Settings for each received project:
  - PLC project name.
  - Hash sum of the PLC project.
  - Modification date and time.
- Settings for each software component in the PLC project:
  - Type.
  - Name.
  - Settings that specify the address of the location in the software component memory.
  - Settings that specify the checksums of the software component.

Commands used for scanning Linux devices in security audit jobs.

When scanning devices running Linux operating systems as part of vulnerability and compliance audit jobs or configuration control jobs, the necessary data is obtained on each device using the commands to start the following utilities:

- blkid
- cat
- df

- dmidecode
- ethtool
- free
- hwinfo
- ip
- ls
- lsblk
- lshw
- lsusb

All of the above utilities must be installed and available in the device operating system. If a utility is missing, data that can be provided only by this utility cannot be received.

All of the above utilities are preinstalled by default in most operating systems supported by Kaspersky Industrial CyberSecurity for Linux Nodes. You can check for the utilities by running the appropriate commands in the console of the device operating system.

To check for the utilities in CentOS:

1. In the computer's operating system console, run the following command:

   ```
   which blkid cat df dmidecode ethtool free hwinfo ip ls lsblk lshw lsusb
   ```

   A list of paths to files of installed utilities will be displayed.

2. Make sure the list contains the paths for all required utilities.

If a utility is missing, install a package containing this utility.

To install the dmidecode package in CentOS,

in the computer's operating system console, run the following command:

```
sudo dnf install dmidecode
```

Device operating systems supported to perform active polling of devices

This article lists the device operating systems supported by the application for active polling of devices.

Windows operating systems

Kaspersky Industrial CyberSecurity for Networks supports active polling of devices running the following versions of Windows:

- Desktop operating systems:
  - Windows XP Professional SP2 x86/x64
  - Windows XP Professional SP3 x86
  - Windows Vista® SP2 x86/x64
  - Windows 7 Enterprise SP1 x86/x64
  - Windows 7 Professional SP1 x86/x64
  - Windows 7 Ultimate SP1 x86/x64
  - Windows 8 Enterprise x86/x64
  - Windows 8 Pro x86/x64
  - Windows 8.1 Enterprise x86/x64
  - Windows 8.1 Pro x86/x64
  - Windows 10 LTSC 2015, version 1507 x86/x64
  - Windows 10 LTSC 2016, version 1607 x86/x64
  - Windows 10 Education RS4, version 1803 x86/x64
  - Windows 10 Enterprise RS4, version 1803 x86/x64
  - Windows 10 Home RS4, version 1803 x86/x64
  - Windows 10 Pro RS4, version 1803 x86/x64
  - Windows 10 Education RS5, version 1809 x86/x64
  - Windows 10 Enterprise RS5, version 1809 x86/x64
  - Windows 10 Home RS5, version 1809 x86/x64
  - Windows 10 Pro RS5, version 1809 x86/x64
  - Windows 10 LTSC 2019, version 1809 x86/x64
  - Windows 10 Education 19H1, version 1903 x86/x64
  - Windows 10 Enterprise 19H1, version 1903 x86/x64

- Windows 10 Home 19H1, version 1903 x86/x64
- Windows 10 Pro 19H1, version 1903 x86/x64
- Windows 10 Education 20H1, version 2004 x86/x64
- Windows 10 Enterprise 20H1, version 2004 x86/x64
- Windows 10 Home 20H1, version 2004 x86/x64
- Windows 10 Pro 20H1, version 2004 x86/x64
- Windows 10 Education 20H2, version 2009 x86/x64
- Windows 10 Enterprise 20H2, version 2009 x86/x64
- Windows 10 Home 20H2, version 2009 x86/x64
- Windows 10 Pro 20H2, version 2009 x86/x64
- Windows 10 Education 21H1, version 21H1 x86/x64
- Windows 10 Enterprise 21H1, version 21H1 x86/x64
- Windows 10 Home 21H1, version 21H1 x86/x64
- Windows 10 Pro 21H1, version 21H1 x86/x64
- Windows 10 Education 21H2, version 21H2 x86/x64
- Windows 10 Enterprise 21H2, version 21H2 x86/x64
- Windows 10 Home 21H2, version 21H2 x86/x64
- Windows 10 Pro 21H2, version 21H2 x86/x64
- Windows 10 Education 22H2, version 22H2 x86/x64
- Windows 10 Enterprise 22H2, version 22H2 x86/x64
- Windows 10 Home 22H2, version 22H2 x86/x64
- Windows 10 Pro 22H2, version 22H2 x86/x64
- Windows 10 LTSC 2021, version 21H2 x86/x64
- Windows 11 Education 21H2, version 21H2 x64
- Windows 11 Enterprise 21H2, version 21H2 x64
- Windows 11 Home 21H2, version 21H2 x64
- Windows 11 Pro 21H2, version 21H2 x64
- Windows 11 Education 22H2, version 22H2 x64

    - Windows 11 Enterprise 22H2, version 22H2 x64
    - Windows 11 Home 22H2, version 22H2 x64
    - Windows 11 Pro 22H2, version 22H2 x64
- Server operating systems:
    - Windows Server® 2003 Enterprise SP1 x86/x64
    - Windows Server 2003 Standard SP1 x86/x64
    - Windows Server 2003 Enterprise SP2 x86/x64
    - Windows Server 2003 Standard SP2 x86/x64
    - Windows Server 2003 Enterprise R2 x86/x64
    - Windows Server 2003 Standard R2 x86/x64
    - Windows Server 2008 Enterprise SP2 x86/x64
    - Windows Server 2008 Standard SP2 x86/x64
    - Windows Server 2008 R2 Enterprise SP1 x86/x64
    - Windows Server 2008 R2 Standard SP1 x86/x64
    - Windows Server 2012 Datacenter x64
    - Windows Server 2012 Essentials x64
    - Windows Server 2012 Foundation x64
    - Windows Server 2012 Standard x64
    - Windows Server 2012 R2 Datacenter x64
    - Windows Server 2012 R2 Essentials x64
    - Windows Server 2012 R2 Foundation x64
    - Windows Server 2012 R2 Standard x64
    - Windows Server 2016 Datacenter, version 1709 x64
    - Windows Server 2016 Essentials, version 1709 x64
    - Windows Server 2016 Standard, version 1709 x64
    - Windows Server 2016 Datacenter, version 1803 x64
    - Windows Server 2016 Essentials, version 1803 x64
    - Windows Server 2016 Standard, version 1803 x64

- Windows Server 2019 Datacenter, version 1809 x64
- Windows Server 2019 Essentials, version 1809 x64
- Windows Server 2019 Standard, version 1809 x64
- Windows Server 2019 Datacenter, version 1903 x64
- Windows Server 2019 Essentials, version 1903 x64
- Windows Server 2019 Standard, version 1903 x64
- Windows Server 2019 Datacenter, version 1909 x64
- Windows Server 2019 Essentials, version 1909 x64
- Windows Server 2019 Standard, version 1909 x64
- Windows Server 2019 Datacenter Core, version 2004 x64
- Windows Server 2019 Standard Core, version 2004 x64
- Windows Server 2019 Datacenter Core, version 20H2 x64
- Windows Server 2019 Standard Core, version 20H2 x64
- Windows Server 2022 Datacenter Core, version 21H2 x64
- Windows Server 2022 Standard Core, version 21H2 x64

- Embedded operating systems:
  - Windows XP Embedded SP2 WEPOS x86/x64
  - Windows XP Embedded SP3 x86 (POS Ready 2009)
  - Windows Embedded 7 SP1 x86/x64 (POS Ready 7)
  - Windows Embedded 8.0 Industry Pro x86/x64
  - Windows Embedded 8.1 Industry Pro x86/x64
  - Windows 10 IoT Enterprise 21H1 x86/x64
  - Windows 10 IoT Enterprise 21H2 x86/x64
  - Windows 10 IoT Enterprise 22H2 x86/x64
  - Windows 10 IoT Enterprise, version 1803 x86/x64
  - Windows 10 IoT Enterprise, version 1809 x86/x64
  - Windows 10 IoT Enterprise, version 1903 x86/x64

- Windows 11 IoT Enterprise, version 21H2 x64
- Windows 11 IoT Enterprise, version 22H2 x64

Linux operating systems

Kaspersky Industrial CyberSecurity for Networks supports active devices with the following versions of Linux:

- 32-bit operating systems:
  - Debian GNU / Linux 10.1
  - Debian GNU / Linux 11
- 64-bit operating systems:
  - AlmaLinux OS 8
  - AlmaLinux OS 9
  - ALT Linux 8 SP Workstation
  - ALT Linux 8 SP Server
  - ALT Linux Workstation 10
  - ALT Linux Server 10
  - AlterOS® 7.5
  - Astra Linux 1.4
  - Astra Linux Common Edition (regular update 2.12)
  - Astra Linux Special Edition RUSB.10015-01 (regular update 1.5)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.7)
  - Astra Linux Special Edition RUSB.10015-16 (version 1) (regular update 1.6)
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.8)
  - Astra Linux Orel 2.12
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.5 (kernel version 2.6.32-432)

- CentOS 6.6
- CentOS 6.7
- CentOS 7.2
- CentOS 8.0
- CentOS Stream 9
- Debian 4
- Debian GNU / Linux 10.1
- Debian GNU / Linux 11
- EulerOS 2.0 SP5
- Linux Mint 19.2
- Linux Mint 20.3
- openSUSE Leap 15.0
- Oracle® Linux 7.3
- Oracle Linux 8.0
- Oracle Sun Solaris 5.10
- Red Hat® 7.0 Guinness
- Red Hat Enterprise Linux® 6.3
- Red Hat Enterprise Linux 6.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 8.0
- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux Server 5.7
- Red Hat Enterprise Linux Server 6.9
- Red Hat Enterprise Linux Workstation 6.7
- RedOS 7.3
- Rocky Linux™ 8.5
- Ruby duck 5.6 (kernel version 2.6.32.-504)
- SUSE® Linux Enterprise Server 12.5

- SUSE Linux Enterprise Server 15
- Tenix WS (Gentoo family)
- Ubuntu 10.04
- Ubuntu 16.04
- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04
- Ubuntu 20.04 LTS
- Ubuntu 22.04
- Ubuntu 22.04 LTS
- Ubuntu Core
- GosLinux 7.17
- GosLinux 7.2

Detecting attributes and typical device interactions in Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks can detect important information about the infrastructure in the network traffic by passive analysis of the device activities in the industrial network and save information about the detected network devices, their attributes, and interactions.

To ensure that Kaspersky Industrial CyberSecurity for Networks can obtain the most accurate and complete information about the process control system components, their attributes, and typical network interactions, it is recommended to perform various maintenance and routine operations in the control system. These can be any operations considered acceptable. The operations must be safe and must not interrupt or impact the normal technological process by other means.

These operations may include but are not limited to:

- Network device polling.
- Initiating the operations between SCADA servers, Historian, HMI, and PLC.
- Connecting to PLCs and IEDs using the appropriate engineering software.
- Uploading and downloading PLC projects.
- Requesting information about the PLC configurations and firmware versions.

- Restarting SCADA servers, Historian, operator and engineer workstations.
- Restarting PLCs and / or IEDs.

For instructions on how to perform operations, see the software and hardware documentation for your process control system.

Configuring port mirroring for Kaspersky Industrial CyberSecurity for Networks

For correct operation, Kaspersky Industrial CyberSecurity for Networks must receive a copy of network traffic sent from the industrial network switch configured to transmit mirrored network packets to the assigned network port. This technology of network traffic mirroring is called Switched Port Analyzer (SPAN) or Port Mirroring.

For traffic mirroring, you are advised to use an interface that supports the Gigabit Ethernet standard.

When configuring port mirroring, you should configure the network switch settings so that there is no duplication of traffic sent to Kaspersky Industrial CyberSecurity for Networks. Duplicated traffic causes additional consumption of disk space on the application node. If you enable data transmission from all source ports to one destination port, use only one direction: Ingress (reception, rx). Otherwise, the SPAN port will duplicate the traffic of devices that are connected to different ports of the switch and are exchanging data with each other.

This section contains port mirroring configuration examples for several Ethernet switch models that can be used in industrial network infrastructure. You can get similar information about configuring other models of switches in the documentation for your network equipment.

Configuring port mirroring for Cisco Access and Distribution switches

You can configure a SPAN session for Cisco Access and Distribution switches (for example, Cisco Catalyst™ 2960 and Cisco Catalyst 3850) using the switch command line interface. To do this, access the target switch via Ethernet or console port and open the switch management functions. In configuration mode, create a new monitoring session, select the sources for traffic mirroring, set the destination port, and save the configuration.

For more information about configuring port mirroring for Cisco Access and Distribution switches, refer to Cisco hardware documentation.

To configure traffic mirroring for Cisco Access and Distribution switches:

1. Enable the privileged EXEC mode using the following command:

```
enable
```

2. From the privileged EXEC mode, enter the global configuration mode using the following command:

```
conf t
```

3. To view the existing monitor sessions, enter the following command:

```
show monitor session all
```

4. If necessary, delete the existing monitor session:

```
no monitor session <session number>
```

where `<session number>` is the number of the monitor session to be deleted. You can specify a value from 1 to 66. You can use the following keywords instead of the session number:

- `all` – to delete all monitor sessions
- `local` – to delete local monitor sessions
- `remote` – to delete remote monitoring sessions

5. Specify the sources for traffic mirroring:

- If the sources are switch ports, use the following command:

  ```
  monitor session <session number> source interface <source ports>
  ```

  where:

  - `<session number>` – monitor session number
  - `<source ports>` – switch ports for monitoring (you can specify several values separated by commas or as a range).

- If the sources are virtual local networks with specific VLAN IDs, use the following command:

  ```
  monitor session <session number> source vlan <VLAN sources>
  ```

  where:

  - `<session number>` – monitor session number
  - `<VLAN sources>` – VLAN IDs for monitoring (you can specify several values separated by commas or as a range).

6. Specify the destination port:

```
monitor session <session number> destination interface <destination port> encapsulation replicate
```

where:

- `<session number>` – monitor session number
- `<destination port>` – port to which a copy of network traffic will be sent.

7. Return to the privileged EXEC mode using the following command:

```
end
```

8. To check the monitor session configuration, enter the following command:

```
show monitor
```

9. To activate SPAN settings after restarting the switch, save the monitor session configuration to a configuration file:

```
copy running-config startup-config
```

Example of defined values in the sequence of commands

```
enable
conf t
monitor session 1 source interface gigabitethernet0/1 - 23
monitor session 1 destination interface gigabitethernet0/24 encapsulation replicate
end
copy running-config startup-config
```

Configuring port mirroring for Cisco Small Business™ switches

For more information on configuring Cisco Small Business switches, refer to Cisco documentation.

To configure port mirroring for Cisco Small Business switches:

1. Connect to the switch and open port mirroring settings in the switch web interface.
2. Select **Administration** → **Diagnostics** → **Port and VLAN mirroring** section.
3. Add source interfaces and select the destination interface.
4. Save the changes.

Configuring port mirroring for Hirschmann industrial Ethernet switches

For more information about configuring port mirroring for Hirschmann Industrial Ethernet switches, refer to Hirschmann equipment documentation.

To configure port mirroring for Hirschmann Industrial Ethernet switches:

1. Connect to the switch.
2. In the switch web interface, select **Diagnostics** → **Port Mirroring**.
3. As a source, select all the necessary RX and TX ports for ingress and egress monitoring.
4. Select the destination port to be connected to Kaspersky Industrial CyberSecurity for Networks device.
5. To enable mirroring, select **On** in the **Operation** section, and then select **Set**.
   Changes will be applied to the volatile memory (RAM) of the device.
6. To save the changes permanently, open the dialog window and click **Save**.

Configuring port mirroring for Siemens SCALANCE switches

For more information about configuring port mirroring for Siemens SCALANCE switches, refer to Siemens equipment documentation.

To configure port mirroring for Siemens SCALANCE switches:

1. Connect to the switch web interface and select **Layer 2** → **Mirroring**.
2. To create a mirroring session:
   a. Select the **General** tab.
   b. Enable Mirroring.
   c. To create a record in the table, click the **Create** button.
      The session ID is assigned automatically.
   d. In the **Session Type** drop-down list, select the **Port Based** value.
   e. Click the **Set Values** button.
   f. In the **Destination Port** column, select the destination port.
      For example, **P0.8**.
   g. Click the **Set Values** button.
3. Select the **Port** tab.
4. In the **Port** tab follow these steps:
   a. In the **Session ID** drop-down list, select the ID of the session you created earlier in the **General** tab.
   b. To monitor all data traffic of a port, select all the ports in the table in the **Ingress** and **Egress** columns.
   c. Click the **Set Values** button.

Configuring port mirroring for Siemens RUGGEDCOM i800, i801, i802, i803 switches

For more information about configuring port mirroring for Siemens RUGGEDCOM switches, refer to Siemens equipment documentation.

To configure port mirroring for Siemens RUGGEDCOM i800, i801, i802, i803 switches:

1. Connect to the switch web interface.

   Default connection to the device is established via IP address 192.168.0.1/24.

2. Select **Ethernet Ports** → **Configure Port Mirroring**.

3. For the **Port Mirroring** setting, select **Enabled**.

4. Specify the source port number in the **Source Port** setting.

5. For the **Source Direction** setting, select **Egress and Ingress**.

6. Specify the destination port number in the **Target Port** setting.

7. Click the **Apply** button.

Glossary

Account role

Set of access rights that determine the actions available to a user when connected to the application Server. Kaspersky Industrial CyberSecurity for Networks provides the following roles: Administrator, Security Officer, Infrastructure Officer, ICS Officer, and Operator.

Address space (AS)

A network segment defined by the rules that determine sets of addresses, VLAN identifiers, or monitoring points.

ARP spoofing

A technique used by criminals to conduct a "man-in-the-middle" attack on networks that use ARP (Address Resolution Protocol).

Asset Management

Technology for registering events associated with the detection of device information in traffic or in data received from EPP applications (for example, an event for the detection of activity from a previously unknown device).

Command Control

Technology for registering events associated with the detection of system commands for devices in traffic (for example, detection of an unauthorized system command).

CVE

Acronym for Common Vulnerabilities and Exposures. Database of publicly known vulnerabilities and information security risks. Vulnerabilities described in this database are assigned identification numbers in the format CVE-<year>-<number>.

Dedicated Kaspersky Industrial CyberSecurity network

A computer network consisting of computers designed for running applications that are part of the Kaspersky Industrial CyberSecurity solution, and the network equipment that enables interaction between computers. The dedicated network must not be accessible from other networks.

Deep Packet Inspection

Technology for registering events associated with process violations (for example, the set temperature value has been exceeded).

Device

Device that is connected to a computer network and is identified by address information that can be saved in Kaspersky Industrial CyberSecurity for Networks (for example, programmable logic controller, remote terminal, or intelligent electronic device).

Device vulnerability

A defect in device hardware or software that can be exploited by a hacker to impact the operation of the information system or to gain unauthorized access to information.

Endpoint Protection Platform

Technology for registering events associated with threats detected by Kaspersky applications that perform functions to protect workstations and servers (for example, a malware detection event).

Endpoint Protection Platform (EPP)

An integrated system providing comprehensive Endpoint Protection (such as mobile devices, computers or laptops) by using various security technologies. An example of an Endpoint Protection Platform is the solution known as Kaspersky Endpoint Security for Business.

EPP application

An application that is included in the Endpoint Protection Platform (EPP). EPP applications are installed to endpoint devices within an enterprise IT infrastructure (such as mobile devices, computers or laptops). One example of an EPP application is Kaspersky Endpoint Security for Windows included in the EPP solution known as Kaspersky Endpoint Security for Business.

Event

Record containing information requiring the attention of an ICS security officer. Kaspersky Industrial CyberSecurity for Networks saves registered events in the database. To view registered events, you must connect to the application Server. If necessary, you can configure transmission of events to Kaspersky Security Center and recipient systems.

Event correlation rule

Set of conditions for checking sequences of events in Kaspersky Industrial CyberSecurity for Networks. When Kaspersky Industrial CyberSecurity for Networks detects a sequence of events that meet the conditions of an event correlation rule, the application registers an incident.

Event type

Defined set of parameters for registering events in Kaspersky Industrial CyberSecurity for Networks. A unique number (event type code) is assigned to each event type.

External

Technology for registering incidents and events that are received by Kaspersky Industrial CyberSecurity for Networks from recipient systems using Kaspersky Industrial CyberSecurity for Networks API methods.

ICS

Abbreviation for Industrial Control System. A group of hardware and software designed to automate control of process equipment at industrial enterprises.

Incident

In Kaspersky Industrial CyberSecurity for Networks, an incident is an event that is registered when a specific sequence of events is received. Incidents group events that have certain common traits or that are associated with the same process. Kaspersky Industrial CyberSecurity for Networks registers incidents based on event correlation rules.

Industrial network

Computing network that links the nodes of an automated Industrial Control System of an industrial enterprise.

Intelligent electronic device (IED)

A set of devices that ensure timely disconnection of faulty power facilities from the power system, and that perform the necessary actions to ensure normal operation of the power system in automated or semi-automated operating modes.

Interaction Control rule

A description of authorized communications for industrial network devices. When Kaspersky Industrial CyberSecurity for Networks detects network interaction that satisfies an enabled Interaction Control rule, the application does not register an event.

Intrusion Detection

Technology for registering events associated with the detection of traffic anomalies that are signs of an attack (for example, detection of signs of ARP spoofing).

Intrusion Detection rule

A set of conditions used by the Intrusion Detection system to analyze traffic. The rule describes a traffic anomaly that could be a sign of an attack in the industrial network.

IOC

Indicator of Compromise. A set of data on a malicious object or action.

IOC file

File containing a set of IOC indicators that, if matched, the application considers an event to be a detection. The likelihood of detection may increase if the check identifies exact matches of the object data with multiple IOC files.

Kaspersky Industrial CyberSecurity for Networks Sensor

Kaspersky Industrial CyberSecurity for Networks component. A sensor is installed on a separate computer (not on the computer that performs functions of the Kaspersky Industrial CyberSecurity for Networks Server). A sensor receives and analyzes data from computer networks that are connected to the network interfaces of the sensor's computer. To receive and analyze industrial network traffic, monitoring points must be added to the network interfaces. A sensor forwards the data analysis results to the Server.

Kaspersky Industrial CyberSecurity for Networks Server

Kaspersky Industrial CyberSecurity for Networks component. The Server receives data, processes it, and provides it to users of the application. The Server can receive data from sensors or independently obtain and analyze data from computer networks that are connected to the network interfaces of the Server computer.

Link on the network map

Object on the network map represented by a line linking the nodes. On the network interaction map, shows the interaction of nodes. On the topology map, shows the physical connection of nodes.

Manageable connector

A software module for data exchange with the application; it provides automatic registration, startup, and control capabilities. Only nodes that have application components installed can serve as deployment nodes for manageable connectors.

Monitoring point

A point where incoming data is received. It is added to the network interface of a node hosting the Server or sensor of Kaspersky Industrial CyberSecurity for Networks, and is used for receiving a copy of industrial network traffic (for example, from a network switch port configured to transmit mirrored traffic).

Network Anomaly Detection rule

A set of conditions for analyzing the attributes of protocols in traffic for the purpose of detecting anomalies that may be indistinguishable from the normal activity of devices at the network level. When a rule is triggered, Kaspersky Industrial CyberSecurity for Networks registers an event.

Network behavior deviations

Network interactions between devices that have resulted in event enrollment due to non-compliance with the enabled Interaction Control rules. Based on network behavior deviation events, you can fine-tune the Interaction Control that is applied to individual devices.

Network Integrity Control

Technology for registering events associated with industrial network integrity or the security of communications (for example, detection of communication between devices over an unauthorized protocol).

Network interaction map

Model that visually represents detected communications between devices. The network interaction map contains the following objects: nodes corresponding to devices, device groups, and links between nodes/device groups.

Node

Computer on which a Kaspersky Industrial CyberSecurity for Networks Server or sensor is installed, or an object on the network map representing one or multiple devices.

PLC project

Microprogram written for a PLC. It is stored in PLC memory and is run as part of the industrial process that uses the PLC. A PLC project may consist of blocks that are individually transmitted and received over the network when the project is read or written.

Process Control rule

A set of conditions for tag values. When the conditions of a Process Control rule are fulfilled, Kaspersky Industrial CyberSecurity for Networks registers an event.

Programmable Logic Controller (PLC)

Industrial controller used to automate enterprise processes.

Risk

A potential threat to the information system resources detected when analyzing traffic and device information.

Risk type

Defined set of parameters for registering risks in Kaspersky Industrial CyberSecurity for Networks. A unique number (risk type code) is assigned to each risk type.

SCADA

Abbreviation for Supervisory Control And Data Acquisition. A software suite that enables the operator to control industrial processes in real time.

Security policy

Set of data that determines the operational settings of Kaspersky Industrial CyberSecurity for Networks.

SIEM

Abbreviation for Security Information and Event Management. This is a solution for managing information and events in an organization's security system.

Single Sign-On (SSO) technology

Mechanism that allows a user to access multiple software resources using the same user account.

System command

Data block in industrial network traffic containing a control command (for example, START PLC) or a system message related to device operation or containing packet analysis results (for example, REQUEST NOT FOUND).

Tag

Variable that contains the value of a specific process parameter such as temperature.

Topology Map

A model for visual representation of the scheme of physical connections between devices in the industrial network. The topology map contains the following objects: nodes representing devices and network equipment, and links representing physical connections of the nodes.

Unmanaged connector

Manually controlled software module for data exchange with the application.

Unmanaged switch

A device without address information for which connections on the topology map are detected or are potentially available.

Information about third-party code

Information about third-party code is contained in the file named legal_notices.txt in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Flash are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

BACnet is a registered trademark of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

Apache is either a registered trademark or a trademark of the Apache Software Foundation in the United States and/or other countries.

iPad, iPhone, Mac, Mac OS, macOS, and OS X are trademarks of Apple Inc.

AXIS and AXIS COMMUNICATIONS are registered trademarks or trademark applications of Axis AB in various jurisdictions.

BitTorrent is a trademark of BitTorrent, Inc.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu and LTS are registered trademarks of Canonical Ltd.

Cisco, Cisco AnyConnect, Cisco Catalyst, Cisco Small Business, Aironet, AnyConnect, IOS, and Jabber are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

Dropbox is a trademark of Dropbox, Inc.

Radmin is a registered trademark of Famatech.

Fortinet, FortiGate, and FortiOS are either registered trademarks or trademarks of Fortinet, Inc. in the United States and/or other countries.

FreeBSD is a registered trademark of The FreeBSD Foundation.

General Electric and Multilin are registered trademarks of General Electric Company.

Google, Android, Chrome, Chromium, Google Chrome, and Nexus are trademarks of Google LLC.

OPPO is a trademark or registered trademark of Guangdong OPPO Mobile Telecommunications Co., Ltd.

HL7 is a registered trademark of Health Level Seven International and its use does not constitute endorsement by HL7.

Hitachi is a trademark of Hitachi, Ltd.

HUAWEI and EulerOS are trademarks of Huawei Technologies Co., Ltd.

Intel, Atom, Core, and Itanium are trademarks of Intel Corporation or its subsidiaries.

IBM and DB2 are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Node.js is a trademark of Joyent, Inc.

Juniper is a trademark or registered trademark of Juniper Networks, Inc. in the United States and other countries.

Linux is the registered trademark of Linus Torvalds in the United States and other countries.

Microsoft, Active Desktop, Active Directory, ActiveX, AppLocker, Authenticode, BitLocker, BizTalk, Cortana, InPrivate, Internet Explorer, Microsoft Edge, Outlook, PowerShell, SmartScreen, SpyNet, SQL Server, Visual Basic, Visual FoxPro, Win32, Windows, Windows Media, Windows PowerShell, Windows Server, Windows Store, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

MOXA is a registered trademark of Moxa Inc.

Mozilla and Firefox are trademarks of the Mozilla Foundation in the United States and other countries.

DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information.

KALI LINUX is a trademark of OffSec.

ONVIF is a trademark of ONVIF, Inc.

OpenSSL is a trademark of the OpenSSL Software Foundation.

OpenVPN is a registered trademark of OpenVPN, Inc.

Oracle, Java, JavaScript, and Solaris are registered trademarks of Oracle and/or its affiliates.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, and Fedora are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Remote Utilities is a registered trademark of Remote Utilities LLC in the United States and/or other countries.

The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

SAMSUNG is a trademark of Samsung Electronics Co., Ltd in the United States or other countries.

Schneider Electric is a trademark of Schneider Electric.

Sendmail and other names and product names are trademarks or registered trademarks of Sendmail, Inc.

Siemens, Simatic, and WinCC are registered trademarks of Siemens AG.

Ruggedcom is a trademark of Siemens Canada Limited.

OpenWRT is a trademark of Software Freedom Conservancy (SFC). Kaspersky Industrial CyberSecurity for Networks is not affiliated with OpenWrt.

Debian is a registered trademark of Software in the Public Interest, Inc.

Dameware is a trademark owned by SolarWinds Worldwide, LLC or its affiliates and registered with the United States Patent and Trademark Office, and possibly registered or pending registration in other countries.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

OpenAPI is a trademark of The Linux Foundation.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

The names, images, and logos that identify UserGate products and services are trademarks of UserGate and/or its subsidiaries or affiliates, and these products are the property of UserGate.

VMware is a registered trademark and/or trademark of VMware, Inc. in the United States and other countries.

VxWorks is a registered trademark (®) or service mark (SM) of Wind River Systems, Inc. This product is not affiliated with, endorsed, sponsored, supported by the owners of the third-party trademark mentioned herein.

ClickHouse is a trademark of YANDEX LLC.

MITRE Corporation Terms of Use

LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.

"© 2025 The MITRE Corporation. This work is reproduced and distributed with the permission of the MITRE Corporation."

DISCLAIMERS

MITRE does not claim ATT&CK enumerates all possibilities for the types of actions and behaviors documented as part of its adversary model and framework of techniques. Using the information contained within ATT&CK to address or cover full categories of techniques will not guarantee full defensive coverage as there may be undisclosed techniques or variations on existing techniques not documented by ATT&CK.

ALL DOCUMENTS AND THE INFORMATION CONTAINED THEREIN ARE PROVIDED ON AN "AS IS" BASIS AND THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE MITRE CORPORATION, ITS BOARD OF TRUSTEES, OFFICERS, AGENTS, AND EMPLOYEES, DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.